Computers & Security 160 (2026) 104705

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

Inside ransomware groups: An analysis of their origins, structures, and dynamics

Andrew Phipps [a], Jason R.C. Nurse [b,*]

[a] School of Computing, University of Kent, UK
[b] School of Computing and Institute of Cyber Security for Society (iCSS), University of Kent, UK

ARTICLE INFO

Keywords:
Cybersecurity
Information security
Ransomware
Cybercriminal profiling
Conceptual framework
Threat actors
Social aspects
Group dynamics
Ransomware gangs
Malware
Qualitative data analysis
Systematic analysis

ABSTRACT

Ransomware is a major cybersecurity threat facing organisations worldwide and has evolved into a highly lucrative criminal enterprise. Over the past five years, Conti, LockBit, and BlackCat/ALPHV have emerged as three of the most prominent ransomware groups, responsible for major cyberattacks across sectors including healthcare, banking, and critical national infrastructure. While these groups are well-known by name and have been discussed in industry articles, blogs, and government briefs, there remains a notable lack of *academic research* into the groups themselves, particularly regarding their origins, values, membership, and organisational structures. This paper addresses this research gap and aims to advance academic understanding of these and other ransomware threat actors, contributing to the evidence base through which they may be better understood and disrupted. Drawing on the PRISMA systematic review approach and a critical analysis of over 500 dispersed sources, including ransomware group communications, we examine the origins, structure, organisation, dynamics and nature of Conti, LockBit, and BlackCat/ALPHV. Our findings reveal that, while each group is unique, they share several noteworthy similarities: Russian origins, business-like operations, an emphasis on brand-building, strong leadership structures, a propensity for retaliation, use of ransomware-as-a-service models, and deployment of multi-level extortion tactics. These insights provide an evidence-based understanding of how such groups function and compare, while also offering important leads for wider mitigation strategies. Consequently, we make several actionable recommendations to disrupt the ransomware ecosystem including undermining ransomware group branding, targeting affiliate networks, and publicly exposing key members. To our knowledge, this is the first academic study to leverage an understanding of these groups, to synthesise such an extensive body of dispersed material, and to apply robust qualitative methods to derive comparative insights for the security research community. In addition, we leverage our findings to introduce a new conceptual framework through which other ransomware groups can be studied, profiled, and compared in the future.

1. Introduction

Ransomware is a type of malware that denies access to data and/or computer systems unless a ransom is paid. It can also involve the exfiltration of data from a system and threats to leak that data if its perpetrator's demands are not met. Over the last five years, ransomware has become a significant cybersecurity problem for organisations around the world. A successful ransomware attack places victims in the difficult situation of being unable to conduct their usual business and exposes them to an extensive range of harms (Mott et al., 2024; Zimba and Chishimba, 2019). One example of a high-profile ransomware incident is DarkSide's attack on Colonial Pipeline which led to a large U.S. pipeline, responsible for transporting 45 % of the East Coast's fuel, shutting down (Abrams, 2021a). Hospitals, airports, law enforcement and other critical infrastructure relied on this pipeline and likely as a result, a ransom of $4.4 million was paid to DarkSide in order to restore the pipeline quickly and safely (The Guardian, 2021). More recent instances of significant attacks include: SafePay's breach of global IT company Ingram Micro (Greig, 2025a); Qilin's attack impacting several London NHS hospitals (Abdul and Milmo, 2024); Scattered Spider's use of DragonForce ransomware against Marks & Spencer (Abrams, 2025); and statewide breaches of Nevada and Minnesota government systems (Gutierrez, 2025).

The impact and money-making potential of ransomware has given

* Corresponding author at: Affiliation: School of Computing and Institute of Cyber Security for Society (iCSS), University of Kent, UK.
E-mail address: j.r.c.nurse@kent.ac.uk (J.R.C. Nurse).

https://doi.org/10.1016/j.cose.2025.104705
Received 14 March 2025; Received in revised form 29 August 2025; Accepted 9 October 2025
Available online 11 October 2025

rise to the formation of a plethora ransomware groups and associated threat actors. Aspects of ransomware attacks have also evolved with many groups now following a ransomware-as-a-service (RaaS) business model (Oz et al., 2022). RaaS involves a core group developing the ransomware and offering the use of it, and support for it, as a service that individual criminal actors known as "affiliates" can pay to use in cyber-attacks. The earnings from attacks are then split between the affiliate and the core group. This allows affiliates to conduct attacks using existing ransomware rather than needing the technical expertise to build their own.

To better cope with the threat of ransomware to the security of organisations, governments and society, it is critical that we increase understanding of the groups and individuals perpetrating these attacks. Doing so would provide crucial insights that could then enable improved capability to defend against and disrupt their activities (Mavroeidis et al., 2021; UK Government, 2023, 2025). This, however, is naturally difficult due to their secretive nature and use of the dark web to obfuscate their actions (Deslandes and Corvin, 2022). It becomes even more difficult to thoroughly study these threat actors when new groups constantly emerge, and old groups rebrand or split into smaller factions (Krebs, 2021; Scroxton, 2024).

In recent years, there have been significant breakthroughs in into behind-the-scenes operations of ransomware groups. In February 2022, Russia began its full-scale invasion of Ukraine and on February 25th, Conti, one of the most prolific ransomware groups of the previous 18 months, made an announcement stating that it supported the invasion of Ukraine (Meegan-Vickers, 2023). This statement was controversial as it aligned Conti with the stance of the Russian government and also consequently made the group a target for pro-Ukrainian hackers and members who were against the invasion. Two days later, a Twitter/X user called @ContiLeaks leaked a substantial amount of insider information about Conti's operations, including chat logs and source code (DiMaggio, 2023a; Flashpoint, 2022). Believed to be from a disgruntled affiliate, this leak exposed communications spanning several years and earned it the nickname the "Panama Papers of Ransomware".

While uncommon, the small number of information leaks from ransomware groups has presented a unique opportunity for cybersecurity researchers. Through analysis of leaked data, industry-based researchers have been able to identify key group members, significant job roles, how groups are structured, and the relationship between their members (CheckPoint, 2022a). Public messages from groups (e.g., intentional announcements) and law enforcement agency (LEA) action (e.g., takedown operations) can also provide insights into their organisation, opinions and membership. For example, reviewing communications on dark web forums provided insight into the LockBit group's leadership (notably the vocal persona of LockBitSupp), its dynamics, and even its relationship with other groups (e.g., DarkSide) (DiMaggio, 2023a). Law enforcement's takedown of LockBit in February 2024 was particularly significant as well because it resulted in the identification of a person behind LockBitSupp and several of the group's affiliates, while also detailing information about the inner operations of the group (National Crime Agency (NCA), 2024a; 2024b). Such developments are essential in the ongoing fight against ransomware.

This paper seeks to advance current research by contributing to the understanding of ransomware groups. While there has been an increasing amount of information on these groups exposed online through data leaks, announcements, industry analyses and LEA operations as discussed above, the opportunity to gather critical insights from this data has rarely been seized in *academic study*. The reality is that these sources often remain dispersed and disjointed and therefore by themselves do little to advance academic scientific research into the inner workings of ransomware groups.

Our research targets this gap and seeks to engage in a comprehensive analysis of ransomware groups by leveraging the aforementioned data. The aim is to investigate the origins, structure, organisation, dynamics and nature of ransomware groups and provide insights that could form the basis for how ransomware groups and the threat that they pose can be tackled. We scope our work to these five areas due to their prominence as key characteristics of groups (Brown and Pehrson, 2019; Ouellet, and Hashimi, 2019; Nurse and Bada, 2018) and the dearth of academic contributions pertaining to ransomware groups in these domains. We draw on a range of primary and secondary data available online as the foundation for our research and consolidate these into insights and themes which can then be used to characterise aspects of the group and inform in making recommendations for the security community.

This study will focus on three of the most prominent ransomware groups from the last five years to help define the inner workings of such entities. We investigate Conti, LockBit and BlackCat/ALPHV. These groups have been recognised as the most active and threatening, often featuring at the top of various trend reports (Kaspersky, 2024a; Borges, 2024; Grossman and Smith, 2024; TrendMicro, 2022a). Even LockBit, which was publicly taken down by law enforcement in 2024 appears to have bounced back and arguably still remains significant actor in the ransomware landscape. Another reason for their selection is that these groups suffered significant incidents. These span the Conti Leaks, the takedown of LockBit and exposure of LockBitSupp's identity, and the law enforcement action against BlackCat/ALPHV and its supposed takedown and exit scam (Ilascu, 2024). This makes them particularly ideal for research into the origins, structure and dynamics given the now-increased accessibility of information about them online and the ability to reflect upon how they have responded to such incidents.

The contributions of this article are therefore as follows. The primary contribution is that, to our knowledge, this is the first academic study: (1) to investigate and compare the inner workings of these three groups; (2) to aggregate such a wide body of dispersed sources (similar in approach to systematic reviews e.g., Patterson et al. (2023)) on this topic; (3) to analyse them using robust qualitative methods to extract empirical insights (e.g., on how groups function, their similarities and differences, and the role of factors such as brand and leadership) for the academic community; and (4) consequently, to build the related evidence base on a topic that is often anecdotally discussed within academic research. In addition, we use insights from our analysis to present actionable recommendations for addressing the ransomware threat.

The secondary contribution of this study capitalises on the opportunity to leverage our qualitative analysis of three ransomware groups. Specifically, it uses the insights and structure derived from this analysis to develop an initial conceptual framework intended to support future analyses of other ransomware threat actors. Through our research, we noticed a significant need for, and value in, such a framework to enable more structured analyses of these groups. Accordingly, we propose this framework as a theoretical contribution of our study.

2. Literature review

There is a wealth of research on ransomware. Three of the primary areas studied are its evolution over time, technical research into how ransomware works and can be defended against, and the impact that ransomware has had on victims. Oz et al. (2022) presents a comprehensive review of these topics including specific focus on its origins, how attack methods and encryption techniques have developed over time, known ransomware families and characteristics, and detection and recovery methods. McIntosh et al. (2024) builds on these points and critically evaluates over 200 ransomware studies and looks at them in relation to existing mitigation strategies and intelligence. It was found that studies were becoming outdated, and that research ought to carefully consider the continuing changes in the industry to stay relevant.

While technical research on ransomware, such as analysing strains, encryption algorithms, and mitigation strategies, has increased over time (Kerns et al., 2021; Kim et al., 2022; McIntosh et al., 2024), the study of ransomware groups themselves has received less attention. Of the research that has explored groups, much of it adopts a conceptual

approach to their analysis. Whelan et al. (2024) compare aspects of ransomware groups with aspects of traditional forms of organised crime such as mafia groups and make the argument that the term "organised crime" should be reconceptualised to include cybercriminal groups such as ransomware gangs. Martin and Whelan (2023) examine the concept of "cyber-privateers" and liken ransomware groups to historical pirates and privateers engaged in acts of state-endorsed crime to increase understanding of the operation of ransomware groups and their relationships with states. Two ransomware groups that appear to be associated with the Russian state, DarkSide and REvil, are analysed specifically and their actions and relationship with Russia are compared to the actions of pirates and privateers and their relationships to states that privateers were affiliated with (Martin and Whelan, 2023).

Increasing understanding of ransomware groups in order to be better prepared in dealing with attacks is a common element of the literature. Boticiu and Teichmann (2023) give an overview and analysis of the process of negotiating with ransomware groups, a topic that they state is not very widely covered in literature. They discuss several aspects of ransomware negotiation that are useful for victims to understand. For example, knowing about if groups have a track record for lowering ransom amounts or if they follow through on their word after receiving ransom payments. Meurs et al. (2022) also explore this topic and show that the ransomware group's efforts and victim characteristics (e.g., industry sector) contribute to ransom amounts demanded and financial losses experienced.

Connolly et al. (2023) investigate the justification that ransomware groups themselves use for their actions. This was completed through the analysis of secondary data and the application of neutralisation theory; i.e., the idea that a person can justify and protect themselves from blame for actions that are not socially accepted (such as breaking the law). It enables criminals to feel less guilty and assume their actions have had less of a significant impact on others. They find that techniques used by criminals include denial of victim, denial of injury and claim of relative acceptability. A unique approach to analysing ransomware groups is adopted by Matthijsse et al. (2023). Their work draws on crime script analysis using court documents and expert interviews to identify how groups initially meet, organise and plan attacks. A primary finding of that study was the professionalism of part of the ecosystem.

Specific ransomware groups have also featured in research, albeit in a limited way. A key factor undoubtedly is the lack of accessible data on these groups and their internal operations and structures. Gray et al. (2022) offers one of the most detailed studies to date with an in-depth analysis of the Conti group. They conduct a qualitative analysis of the messages exposed in the Conti Leaks to provide further insight into topics such as its origins, team composition (with the number of people in various teams and the associated salaries), and situations where employees were unaware that they were working for a ransomware group. It also includes an analysis of cryptocurrency addresses associated with Conti that is then used to estimate salaries, operating costs, revenue and techniques used in cashing out.

Ruellan et al. (2024) analyse Conti based on the Leaks and conclude that it functions akin to an ordinary large business in the sense that its operations required a non-technical workforce with a variety of different skills that ordinary companies value (such as customer service and management skills). Paternoster et al. (2024) also investigate the group's internal dynamics though through the use of social network analysis and qualitative content analysis. Similarly, they find that Conti is structured comparable to an ordinary large business with a division of labour. They also note that Conti's high-level managers engage closely with group members which they state differs to prior research into traditional criminal groups and may result from the online aspect of their operation. Outside of the aforementioned articles and a few others (e.g., Mersinas et al., 2024; Martin et al., 2024), which are all limited in group scope and characteristics studied, there has been little academic research to understand these groups.

This paper therefore seeks to further understanding of ransomware groups, with a specific focus on the internal aspects of groups themselves. This builds on current research, such as the work above on Conti (which largely exists due to the Conti Leaks), but seeks to broaden that scope to other groups, namely LockBit and BlackCat/ALPHV, which are not as prevalent in the *academic* literature. Through a comprehensive analysis of available primary and secondary data on these groups, we aim to extract insights that can be used to characterise groups and define their origins, structure, organisation, dynamics and nature. As can be seen from our review above, these five areas are not ones that feature prominently in the existing research across multiple ransomware groups. Moreover, these areas are particularly relevant as they are often studied and discussed as key characteristics of groups generally. Prior research into groups that spotlight these areas includes: Brown and Pehrson (2019) who consider general group origins, organisation and dynamics, and Ouellet and Hashimi (2019) and Nurse and Bada (2018) who examine origins, structure and nature especially for criminal groups. In sum therefore, this study will address a key research gap in existent literature on the understanding of such ransomware groups. It also provides a basis for how such groups may be compared, and more generally, will create a foundation that could inform evidence-based ransomware mitigation efforts.

3. Methodology

To achieve the primary aim of this research and thereby elucidate the inner workings of ransomware groups, we adopted a methodology consisting of three stages.

The first stage involved identifying and collecting pertinent data on the selected groups. To ensure a scientific and robust approach was followed, we adopted the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) technique (PRISMA, 2020). PRISMA is a well-recognised method for conducting systematic reviews of a topic, including identifying, extracting and synthesising findings in a transparent and repeatable way (Page, 2021; Patterson et al., 2023). The process began by defining a search query that would be used to locate the necessary data. We used the name of the ransomware group (e.g., 'Conti'), the word 'ransomware', and the AND operator followed by the terms of interest, i.e., 'origins', 'structure', 'organisation', 'dynamics', and 'nature' with OR operators between these. To this base query, we also added other related terms (using the OR operator) that could lead to additional relevant information. Appendix A presents the queries used for each group. These queries were input into Google Search in August 2024 and all results from each Google search were considered; typically, this spanned at least 23 Google Search pages each containing 10 results. Where groups have had aliases, these additional names have also been included in the search.

To identify the most pertinent articles, a set of inclusion and exclusion criteria were defined. The primary inclusion criterion was that the result (i.e., article/source) must relate to, or include information about, Conti's, LockBit's or BlackCat/ALPHV's origins, structure, organisation, dynamics or nature. The exclusion criteria were centred on removing results that were: not in English or not readily accessible; sponsored Google Search results (to avoid potential bias); social media videos (our research is scoped to textual content); or Google Books extracts (due to limited access). As origins, structure, organisation, dynamics and nature are the primary areas of groups that are under investigation in this research, it is important to define and contextualise these. We characterise these areas as follows:

- Origins refers to the beginnings of a ransomware group. This covers country of origin or affiliation and first discovery of the group. It also acknowledges that a group may consist of members that were previously in another ransomware group, or it may have started operating in a certain way or due to a certain cause.
- Structure considers the arrangement of people and roles within the group, including the ransomware working model of the group, how

people are recruited and vetted, and the overall group's management or leadership.
- Organisation speaks to the group's operational setup. For example, how the group distinguishes and promotes itself, its preferred means of extortion, and how payments are received.
- Dynamics refers to changes in operations over time and behaviours in response to certain situations. For instance, changes in ransomware strains, attacks or tactics, and response to law enforcement operations, or the actions of other actors (e.g., disgruntled members).
- Nature captures the typical character or modus operandi of groups and their general behaviours. For example, who they target, their typical activities and any ethical boundaries.

When reviewing each result found, if one or more aspects relating to these five areas as defined were identified (i.e., the inclusion criteria was fulfilled), and the article passed the exclusion criteria screening, the article was included. Specifically, this meant that it was recorded, and the relevant information (e.g., excerpts from the article) was transferred to a data archive corresponding to the groups' origin, structure, organisation, dynamics or nature, respectively. This allowed for information relating to the five areas to be extracted, in preparation for their analysis. If an article did not include information relating to either of the five areas, it was excluded and deemed irrelevant. For instance, an article would be deemed irrelevant if it included the word "structure" but was referring to the structure of the article instead of the structure of the respective ransomware group. The gathering and assessment of results was led by one researcher, whilst a second researcher was responsible for checking that all recorded information fulfilled the inclusion criteria and conducting independent searches (using the defined queries) to ensure that relevant articles were not unduly excluded. In total, there were 551 sources reviewed (see PRISMA flow diagram in Appendix B); approximately 120 of which are directly referenced in this research manuscript.

In the second stage of the study, we engaged in a comprehensive analysis of the collected data. Data was reflexively coded and assessed using the thematic analysis approach developed by Braun and Clarke (2006). This approach has been successfully applied in cybersecurity research and enables primary topics, as well as similarities and differences across the data to be efficiently and effectively defined (Mott et al., 2023; Patterson et al., 2024). A mixed approach utilising both deductive and inductive thematic analysis was implemented; this builds on precedents in research (Braun and Clarke, 2012; Fereday and Muir-Cochrane, 2006). This approach also allows us to take advantage of the benefits of each technique; notably, the structure provided by a deductive analysis and the flexibility of the data-led inductive process.

More specifically, the deductive approach enabled us to establish areas in advance for what the present study sought to understand, i.e., the origins, structure, organisation, dynamics and nature of these groups. As explained in Section 2, this scoping was grounded in theory (i.e., these areas have previously been identified as key characteristics of groups generally) and a lack of research in this space. An inductive thematic analysis approach was then applied to the data within each area and codes were generated inductively and reflexively; this ensured that codes were directly grounded in the data that was gathered. The code book created was then discussed by both researchers and finalised. Researchers then independently coded the data and came together to compare for, and address, any notable variances in the coding results. To assess the level of inter-coder reliability, Cohen's Kappa coefficient was calculated (Bryman, 2016); this yielded a score of 0.87, which indicates a strong level of agreement and matches other, similar research (Ferguson-Walter et al., 2023; Mott et al., 2024). Codes were observed, analysed and collated to generate themes and ultimately, facilitated the discovery of insights across the ransomware groups.

In assessing the information captured, we needed to be cautious about the presence of misinformation, propaganda, outdated data, and contradictory content. To address this concern, once data was gathered and appropriately segmented, we reviewed the information emerging from the various sources and sought to triangulate the resulting insights. Triangulation involved systematically examining the extent to which the data from different sources corroborated (and did not conflict with) each other, and therefore could increase confidence in a particular finding. The timeliness of the source was also an important factor to avoid outdated data. Considering that we are studying criminals who by nature are arguably untrustworthy, in this process we also prioritised data from official sources (e.g., CISA, NCSC, DOJ) and industry-based research studies (e.g., CheckPoint (2022a, 2022b), Krebs (2022), TrendMicro (2024)) to reduce the likely impact of inappropriate data influencing our findings.

The final stage of the methodology drew on the insights from the thematic analysis to produce a profile of each group. The profiles presented summative insights from the data gathered and answered questions such as where the groups originated, how are they structured, and how have they changed due to internal and external pressures. Group profiles were organised such that they covered the primary characteristics of interest (e.g., origin, nature, dynamics) while also enabling comparison of groups. Patterns across the groups were then systematically explored and noted. The general insights and patterns discovered throughout the research provided a sound basis for developing a better understanding of these groups and a pathway to recommendations for their disruption.

The robust methodology outlined above was essential in achieving the primary research contribution and in building the academic evidence base on ransomware groups. A further benefit of this methodology was that it provided a strong foundation for the development of a new conceptual framework grounded in both the approach itself and its outputs, especially the qualitative thematic analyses. This framework offers a tool for researchers and practitioners to understand and profile ransomware groups, in a manner similar to how our study examined Conti, LockBit, and BlackCat/ALPHV. This secondary contribution is presented in more detail in Section 5.4.

In conducting any research, particularly socio-technical studies into criminal entities, an important methodological consideration is ethics. Two primary concerns were identified: the possibility that conducting research into threat actors and their communications may inadvertently promote them and/or their actions; and the reality that this research leverages data that has been leaked, i.e., unduly exposed. In response to the first concern, we acknowledge this here and explicitly state that we do not glorify or promote criminals or their activities. Our research should be viewed as analogous to other works (e.g., NCA (2017), Meland et al. (2020) and Broadhurst et al. (2014)) in this regard and thus focused more on understanding for the purposes of preventing crime. Noting the second concern, we appreciate this fact and have been guided by Boustead and Herr's (2020) guidance on using leaked datasets for research. We underline the fact that this research maximises benefits (e.g., to law enforcement, the security community and society) while minimising harms through its use, and also observe the low risk of individual victimisation as no privately identifiable information is used or exposed.

4. Results

In line with the aim of this research and the areas under study, the findings are organised to present the origins, structure, organisation, dynamics and nature of the Conti, LockBit and BlackCat/ALPHV (hereafter, BlackCat) ransomware groups. We focus on presenting noteworthy insights related to each area and comparing these across groups to understand pertinent similarities and differences. This work is grounded in existing articles and as such, we evidence our findings throughout. For completeness, Appendix C includes the summary table of group aspects linked to themes, while Appendix D outlines the summarised profiles created for each of the groups.

4.1. LockBit, BlackCat/ALPHV and Conti: origins

4.1.1. Association and links to Russia

All three groups were found to have Russian origins, with a majority of sources referring to the groups as Russian, Russian-speaking, associated with Russia, or possessing members or affiliates that are known to be Russian nationals. Specifically, Russian-speaking members were observed in BlackCat (Kovacs, 2023; Tata Communications, 2024), LockBit (Geary, 2023; eSentire, 2023a) and Conti (PSBE Cyber News Group, 2022; Sangfor, 2022) while an association with, or base in, Russia was posited with BlackCat (eSentire, 2023b; Benge, 2023), LockBit (Corera, 2024; Lyngaas, 2024), and Conti (CheckPoint, 2022a; Bing, 2022). Current geographic links to Russia were not unequivocal, however. LockBit members were arrested in the U.S., Canada, Poland, Ukraine (Collier, 2024; Department of Justice (DOJ), 2024) and an individual known to have worked with Conti was arrested in Ukraine (Paganini, 2024). LockBit has publicly claimed on its website that it is "*located in the Netherlands*" (Levison, 2024), but supporting evidence for this claim was not discovered throughout our research.

Notable links to the Russian government were only discovered in the Conti group. This could be seen in its declaration of "*full support for the Russian government*" in February 2022 after Russia's invasion of Ukraine began (Vicens, 2022). Additionally, messages from the Conti Leaks suggests that Conti may have had an arrangement in place with the Russian government that meant that the group would co-operate with the government if they were requested to (Cyberint, 2022). LockBit is not known to be tied specifically to the Russian government (Menn and Sands, 2024) and has stated that they are "apolitical" (Levison, 2024). Similarly, BlackCat is not known to have specific ties to the Russian government (Farrell, 2024).

4.1.2. Successor operations and prior criminal experiences

Two common characteristics between BlackCat and Conti were that both groups were successors to previous ransomware brands and operations, and that members were believed to be experienced criminals. BlackCat first appeared in November 2021 as a rebrand of DarkSide and BlackMatter (Canadian Centre for Cyber Security, 2023) with members from REvil (Barry, 2024a). Conti appeared in 2019 as a successor to Ryuk and is believed to include members from the group behind Trickbot malware (Krebs, 2022; TRM, 2022). LockBit debuted as "abcd" ransomware in 2019 (Sangfor, 2024) but is not known to have originated from a specific previous group. LockBit was, however, observed to recruit affiliates and developers from other ransomware operations such as NoEscape and BlackCat (Rosendahl and Burton, 2024), suggesting that some of its members possess prior criminal experience. The evidence therefore suggests that the groups often tend to originate from earlier ransomware operations or members of the groups have previous cybercriminal experience.

Table 1 shows a summary of some of the key comparisons across the three groups. We also include similar summarised tables in other subsequent sections. These tables are intended to depict a selection of the detailed comparisons made, some of which we then cover in more detail in the present results discourse.

Table 1
Comparing origins of each group.

Theme	BlackCat	LockBit	Conti
Country based in	Russia	Russia	Russia
First appearance	November 2021	September 2019 (abcd)	2019
Predecessor operations	DarkSide, Blackmatter, REvil	N/A	Ryuk, TrickBot, Emotet

4.2. The internal structure of prominent ransomware groups

4.2.1. Business-like structures and functions

The three groups were observed to be similar in structure to that of a regular business. This was particularly evident in their division of work and presence of certain roles; for instance, the groups all possessed structures comparable to a software company with a dedicated team of developers and sales staff. A business-like configuration was especially noticed in Conti as compared to LockBit and BlackCat, due to the large amount of information exposed in the Conti Leaks (CheckPoint, 2022b; Cyberint, 2022; Krebs, 2022; Burgess, 2022a). Research points to it maintaining a business-like hierarchy with multiple teams, a CEO, managers who would check on employees, administrators, developers, testers, and a Human Resources team (CheckPoint, 2022b; Cyberint, 2022; Krebs, 2022; Burgess, 2022a). We were also able to identify visual characterisations and hierarchies of the group's business-like structure (CheckPoint, 2022b; Cyberint, 2022).

Similar to an ordinary business, we found that employees in Conti would receive a regular salary, have working hours, request holiday, and tended to form working relationships with their colleagues (CheckPoint, 2022b; Burgess, 2022). The group even had an "*employee of the month*" scheme, which when awarded came with *"+50% of salary*" (CheckPoint, 2022b; Burgess, 2022a). Despite the similarities to ordinary businesses, there were a number of common elements that were not typical of an upstanding enterprise such as the use of fines to punish employees or the use of pseudonymous usernames by all staff. It was also noted that there were antisemitic remarks and references to child abuse in Conti's messages (Burgess, 2022a); these are sentiments that would not be tolerated in a normal organisation.

Although much less information was available about the structure of BlackCat and LockBit, there was some evidence that their structure was comparable to a traditional business. This particularly linked to their division of labour with different roles; for instance, developers who created and maintained the ransomware strains, and affiliates who would conduct the attacks (Plumb, 2022; TrendMicro, 2022b). Groups, such as LockBit, even attempted to poach developers and affiliates from BlackCat after it was disrupted by the FBI (Rosendahl and Burton, 2024); poaching employees is not an uncommon activity in business more widely (BBC, 2022). It shows that the groups require skilled people employed in different roles in order for their business model to succeed. It also suggests that much like a legitimate business, ransomware groups are competing against one another for talent that can better enable their operations to succeed.

4.2.2. The RaaS model and processes for recruitment, vetting and affiliate status

The RaaS business model was adopted by all the groups studied, and therefore they each had employees internally as well as a set of external affiliates. As in normal RaaS models, we found that the main groups were responsible for developing and maintaining the ransomware while affiliates deployed it against victims. There were differences in the payment structures adopted by groups. For instance, BlackCat affiliates would deploy the ransomware, and the group would pay them up to 90% of the ransom as commission (Krebs, 2023; Center for Internet Security, n.d.). LockBit, on the other hand, allowed affiliates to receive ransom payments directly before the payment of a 20% commission to the main group (Meegan-Vickers, 2024; eSentire, 2023). In the case of Conti, rather than receiving a percentage of the ransom, affiliates were instead paid a set wage (Flashpoint, 2022; Heimdal, 2024). This demonstrates a diversity of operations amongst groups that maps to the wider ecosystem as well.

The groups were found to recruit from cybercrime forums and to have varying rules in place for affiliates and new members; in particular, affiliates and other members underwent forms of vetting and were subjected to rules that had to be followed to remain in good standing with the group. BlackCat affiliates were, for example, interviewed and

vetted before receiving control panel access (Tanner et al., 2022). Multiple sources confirmed that joining Conti involved interviews and may have required the vouch of another criminal (DiMaggio, 2023a, 2023b; Gray et al., 2022).

In some articles, LockBit was said to maintain a more open affiliate program subject to less vetting than other ransomware operations on the basis that the primary requirement to join was to pay enough money (Burgess, 2024). In other sources however, contrary evidence was presented. These suggested that the group had a heavy vetting process in addition to the initial payment. The rationale as stated by LockBit themselves was: "*every candidate to join our affiliate program should understand that we are constantly trying to be hacked and harmed in some way*" (Plumb, 2022). Affiliates, for instance, were required to send proof of previous experience and activities, and had to earn a certain amount of money in Bitcoin each month to maintain their status as an affiliate (Plumb, 2022).

BlackCat had requirements for affiliates to maintain their status and also had perks for high-performing affiliates. Specifically, reports highlighted that underperforming affiliates would be removed from the programme while affiliates who had earned a large amount of money would be granted "Plus" status with access to additional features such as the use of Distributed Denial-of-Service (DDoS) attacks against victims (Symantec, 2022). There was not as decisive information found about Conti regarding affiliates maintaining their status, however, it is clear that certain rules were in place as affiliates were monitored and removed in several cases (Abrams, 2021b; eSentire, 2023).

4.2.3. Strong leadership figures

Both LockBit and Conti possessed prominent leadership figures. "LockBitSupp", now publicly identified as Dmitry Yuryevich Khoroshev, was (and still is) an outspoken chieftain in the group (NCA, 2024b). In Conti, a member called "Stern" has been recognised as a key leader and likened by a number of sources to the CEO of a company (Cyberint, 2022; Burgess, 2022a; CheckPoint, 2022b). Other noteworthy leadership figures include "Professor" (tooted as a senior general), "Tramp" a.k.a. "Trump" (considered a Conti overlord), and "Hof" and "Reverse" (who head hacking/penetration testing teams) (Krebs, 2022). A specific leading member was not discovered for BlackCat.

Analysing the leadership of LockBit in further detail, LockBitSupp served as a major public-facing figurehead and spokesperson. He was observed to communicate with other criminals on cybercrime forums, speak with security researchers and journalists in interviews (Temple-Raston et al., 2024), and announce and host promotional campaigns. In a public interview, when asked if they had a message for the world LockBitSupp simply replied, "*Join my affiliate program and get rich with me*" (Temple-Raston et al., 2024). This was after iterating that they were misidentified as Dmitry Yuryevich Khoroshev and stating that law enforcement action against LockBit "*only motivates me and makes me work harder*".

Stern, on the other hand, maintained a more low-key role and shied away from public interactions. Their position in the group was only apparent due to the leak of internal Conti chat logs (Cyberint, 2022). From these leaks, we were able to uncover a picture of Stern as a "much higher-up", "cantankerous taskmaster" to use the wording of one source (Krebs, 2022). Combining these insights with those from LockBit, these sources depict the two groups' central leaders as strong figureheads.

Table 2 shows a summary of some of the key comparisons across the three groups; the full list can be found in Appendix C.

Table 2
Comparing the internal structure of each group.

Topic of comparison (theme)	BlackCat	LockBit	Conti
Ransomware-as-a Service	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates are paid up to 90 % commission.	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates receive ransom and pay main group 20 % commission.	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates paid a set wage.
Business-like structure	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business.	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business.	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business. Management, HR, Admin teams discovered.
Leadership	No specific leading member identified.	LockBitSupp identified as leader. Public-facing and extroverted persona.	Stern identified as leader. Internally focused personae. Multiple managers with significant roles.

4.3. Group organisation: operational and business setup

4.3.1. Multiple extortion techniques to target victims

The use of multiple levels of extortion was witnessed in the operations of all of the groups studied. Double-extortion, where victim data was both exfiltrated and encrypted, was leveraged by Conti (Fier, 2021), LockBit (CISA, 2023a; 2023b) and BlackCat (TrendMicro, 2022b). Additionally, there were cases where data only was exfiltrated rather than encrypted such as when BlackCat exfiltrated data from Reddit (SOCRadar, 2022). Triple extortion involving the additional threat of a DDoS attack was found in the cases of LockBit (Europol, 2024) and BlackCat (Akamai, n.d.).

Focusing on BlackCat, this threat was taken a step further with quadruple extortion where third-party suppliers of a victim were threatened as well (Jones, 2023; Quorum Cyber, n.d.). BlackCat also utilised extortion through the reporting of a victim to the U.S.' Securities and Exchange Commission (SEC) for not disclosing that they had been breached (Muncaster, 2023). Its public notice about the report stated, "*MeridianLink fails to file with the* SEC*..so we do it for them*" (MalwareHunterTeam, 2023). In this case, they sought to use national incident disclosure regulation as a further threat and means of extortion – this was regarded as a first, and its boldness surprised many in the security industry (SC Media, 2023).

4.3.2. Increasing brand appeal through appealing products and services

As a part of their operations, ransomware groups demonstrated an appreciation for building appealing and easy-to-use products, services and features. The ability to customise ransomware was observed as a means to increase brand appeal to affiliates in BlackCat (Kaspersky, 2024b) and LockBit (Meegan-Vickers, 2024). This included features such as the ability to specify what files to include during encryption and how many layers of extortion were used. We also noted that the ability to target multiple operating systems was prioritised by BlackCat and LockBit, thereby allowing them and their affiliate networks to target a wider proportion of organisations (Tanner et al., 2022; CISA, 2023b). Furthermore, presumably to increase the likelihood of success of receiving ransom payments, leak sites were prominent across all three groups (TrendMicro, 2022a).

Efforts to reduce the technical barrier to entry were discovered as well. LockBit was identified as being easy for potential affiliates to use even without a high degree of technical knowledge (CISA, 2023b; Levison, 2024) and was additionally known for its speed and stealth

(Securin, 2023). This was also the case for BlackCat (Kaspersky, 2024c). Efforts to increase ease of use for affiliates can be seen in how LockBit developed LockBit Green, a version of LockBit based on leaked Conti source code (TrendMicro, 2024), allowing for affiliates familiar with Conti's operation to utilise its features (Meegan-Vickers, 2024). Conti was reported to have sold training documents valued at $1500 for teaching affiliates about ransomware processes (Flashpoint, 2021), suggesting that it believed its knowledge had notable value to potential affiliates. These findings imply that providing an appealing ransomware 'product' that is easy to use was significant as it allowed for the attraction of affiliates that would then contribute to the group's operations.

4.3.3. Advertisements and promotions to grow operations

All three groups were observed to have taken part in activities that involved the advertisement and promotion of their operations and affiliate programmes. This was particularly witnessed on underground forums for BlackCat (Hill, 2023), LockBit (SOCRadar, 2023) and Conti (CheckPoint, 2022b). In Conti, advertisement of jobs took place even on legitimate job sites such as "superjobs.ru" and "headhunter.ru" (CheckPoint, 2022b). A number of promotional campaigns also took place. Technical writing competitions were sponsored by both Lockbit (DiMaggio, 2023b, 2023c) and Conti (Krebs, 2022), and LockBit ran numerous promotional campaigns including paying people for getting LockBit logo tattoos, launching a bug bounty (DiMaggio, 2023b) and offering to pay a reward to anyone who could identify LockBitSupp (NCA, 2024b). This was not witnessed with BlackCat, which appeared to be more conservative in this regard.

Several aspects of the ransomware operations were seemingly deliberately designed to attract potential affiliates. One key example is the way groups structured affiliate payments. As discussed in Section 4.2.2, some groups, such as BlackCat, offered affiliates up to 90% of the ransom as commission. Others, like LockBit, allowed affiliates to collect the ransom first, requesting only 20% as its fee. These different models each offered distinct advantages, appealing to various types of affiliates. Conti's approach was particularly distinctive, offering fixed wages instead of commission-based payments. This model was likely to attract affiliates seeking more stable and predictable income.

Not dissimilar to legitimate businesses (Bhasin, 2011; Nield, 2024), advertising and promotion involved the disparagement of other groups. Conti was found to have accused other groups as being scammers or inexperienced (Kovacs, 2022). Similarly, LockBit ridiculed competing groups to boost its own credibility by comparison (CISA, 2023b; Temple-Raston et al., 2024). In one case, it even insinuated that another group was behind a ransomware attack on a hospital that potentially contributed to the death of a baby (DiMaggio, 2023b). It appears that each group believed that by advertising and promoting themselves, they would be able to attract members who trust their operations to be successful and can therefore continue.

4.3.4. Cryptocurrency as a standard

Cryptocurrency played a key role in the business model of the groups. All three requested their ransoms to be paid using cryptocurrencies and these digital currencies appeared to be standard in group operations (B. Krebs, 2024; NCA, 2024a; Meegan-Vickers, 2023). This was undoubtedly due to its ability to allow for payments to be received in a largely anonymous way. From our analysis, Bitcoin was the most prominent currency and was reported for BlackCat (Martinez, 2022), LockBit (Plumb, 2022), and Conti (Krebs, 2022). In a slight deviation from the norm, we identified an instance where BlackCat was said to offer a payment discount to victims if they used Monero instead of Bitcoin (Martinez, 2022). This likely sought to capitalise on Monero's enhanced privacy protections. Outside of payments, groups also used cryptocurrencies for other purposes. Conti experimented with cryptocurrency-related scams (Krebs, 2022) and LockBit required a Bitcoin deposit to vet that new affiliates were not members of law enforcement or journalists (Plumb, 2022). In sum therefore, cryptocurrency appears to be central in each group and the facilitation of its operations.

Table 3 shows a summary of some of the key comparisons across the three groups; the full list can be found in Appendix C.

4.4. Ransomware groups and their dynamics

4.4.1. Constant development of new and improved ransomware strains

Groups invested significant effort into developing improvements and new versions of their ransomware strains over time. Through regular updates to their methods and tactics, they sought to increase attack success rates and harms, and simultaneously distinguish themselves from other groups. BlackCat has reportedly worked on a version called "Sphynx" with improved speed and stealth capabilities (Akamai, n.d.). LockBit developed numerous new versions as well. It began with abcd, and subsequent versions included LockBit 2.0, LockBit 3.0, LockBit Green (CISA, 2023b) and a version in development called LockBit-NG-Dev (TrendMicro, 2024). Each of these versions possessed new and improved capabilities such as improvements to encryption and stealth (Securin, 2023).

LockBit implemented improvements from other ransomware groups as well. For example, LockBit 3.0 appeared to be influenced by BlackCat ransomware (CISA, 2023b; 2023c) and LockBit Green was reported to be influenced by leaked Conti source code (TrendMicro, 2024). Specifically named versions of Conti were not observed, but the Conti Leaks revealed that the group had employees regularly testing Conti's ransomware and improving it (Krebs, 2022).

4.4.2. Retaliation and responses to perceived injustices

In investigating the dynamics of a ransomware group, a primary topic of consideration is how it behaves in response to actions that threaten it. In our case, all three groups were found to have taken retaliatory action at some stage in their existence. This transpired against law enforcement agencies (LEA), their victims, other cybercriminals, and even their own members.

Reprisal against LEA was witnessed by both BlackCat and LockBit.

Table 3
Comparing each group's organisation and organisational activities.

Topic of comparison (theme)	BlackCat	LockBit	Conti
Advertisement and promotion	Promotion on underground forums. Competitive commission offered (90 %).	Promotion on underground forums. Technical writing contests. Paying people to get LockBit tattoo. Disparagement of other groups. Benefit of receiving ransom payment directly and then paying main group commission.	Promotion on underground forums. Technical writing contests. Disparagement of other groups. Advertisements on legitimate job sites.
Appealing and easy to use product	Highly customisable ransomware. Fast execution. Works across multiple platforms: Windows, Linux. Darknet leak site used. Public data leak site used (likely for added pressure).	Customisable ransomware. Fast execution. Works across multiple platforms: Windows, Linux, MacOS. Darknet leak site used. Automated targeting possible.	Fast execution. Darknet leak site used. Works primarily on Windows. Sold training documents.

Following law enforcement action against BlackCat in December 2023, the group responded by increasing ransom commissions for affiliates to 90% and reducing targeting restrictions on organisations that it claimed were previously off-limits such as nuclear power plants and hospitals (Krebs, 2023). An excerpt from their response statement read: *"As you all know, the FBI got the keys to our blog … Because of their actions, we are introducing new rules, or rather removing ALL the rules except one, you can not touch the CIS, you can now block hospitals, nuclear power plants, anything and anywhere"* (Abrams, 2023; Krebs, 2023).

These actions aimed to increase BlackCat's appeal to affiliates and enable more attacks and greater harms as a means of punishing international LEA action against its activities (Mott et al., 2024). At the same time, it sought to ensure that nations in the Commonwealth of Independent (CIS), i.e., those linked to the former Soviet Union (including Russia, Belarus, Kazakhstan), were not impacted (European Union (EU). (n.d.)). After the takedown of LockBit in February 2024, LockBitSupp responded by seeking initial access brokers with access to government, non-profit and educational organisation websites to carry out new attacks on such entities (Seals, 2024). This was significant because groups were traditionally not openly direct in their targeting.

Retaliation against the actions of victims was seen across all three groups, largely in that the groups would leak or refuse to decrypt data if they were not paid a satisfactory ransom by the victim. In Conti, we found that even if a victim were to pay a ransom, if the victim posted anything from negotiations with Conti, Conti would retaliate by leaking the victim's data anyway and potentially also the data of another victim as well (Flashpoint, 2022). The groups' own members were also subject to punitive actions. LockBit affiliates could be expelled from its affiliate programme if they were determined to have broken the rules; this was aptly seen in their statement apologising for attacking a children's hospital and claiming to have removed the responsible affiliate while also offering a free decrypter to the hospital (eSentire, 2023). Fines were levied against underperforming members in the Conti group as punishment (CheckPoint, 2022b). Additionally, BlackCat suspended one of its affiliates' accounts during its exit scam, demonstrating another way in which these groups could exert authority over members they had disagreements with (Barry, 2024a).

Retaliations targeting other cybercriminals featured in some cases and reports. When LockBitSupp was banned from two prominent Russian-speaking forums, namely XSS and Exploit, they publicly spoke of plans for revenge: "*I'm still looking for the administrator of xss.is. As long as I have several suspects, revenge is inevitable*." (Temple-Raston et al., 2024). It is unclear whether these threats subsequently materialised.

4.4.3. Challenges: to downplay or to embrace?

As seen in the previous section, ransomware groups faced a number of threats, some existential. An interesting observation which we pick up on in this section is cases where they opted to downplay or capitalise on these challenges. Reflecting on the data gathered, the groups responded in similar ways to incidents that negatively affected their operations. Downplaying challenges was especially visible in LockBit's response to its February 2024 LEA takedown and also in BlackCat's reaction to its December 2023 takedown (Secureworks, 2023). In both cases, they made public statements that trivialised the effectiveness of the operations. BlackCat openly stated, "*The maximum that they have is the keys for the last month and a half, it's about 400 companies, but now more than 3000 companies will never receive their keys because of them*" (Secureworks, 2023). This therefore focused more on the larger number of companies who would suffer as a result.

LockBitSupp made numerous statements downplaying the LockBit takedown, including claiming that the takedown happened because they got lazy: "*Over the years my vigilance has relaxed. I got lazy*" (Temple-Raston and Powers, 2024). And, that most LockBit partners still continued to work with it and that they felt LockBit would be fine in the long-term. Additionally, when LEA revealed the identity of a/the person behind the LockBitSupp persona, LockBitSupp went on to claim that law enforcement was mistaken and that they [LockBitSupp] did not know who that person was (Temple-Raston et al., 2024). LockBitSupp also blamed a reduction in attacks on the season – "*Spring is always less productive than winter. This is a seasonal phenomenon*" – rather than the law enforcement takedown (Temple-Raston et al., 2024).

Downplaying law enforcement action was also witnessed in LockBit's actions after its takedown. A new leak site was set up shortly after and new victims were listed; this was as if to demonstrate that its operations were still ongoing. It was later discovered, however, that the number of victims being posted by LockBit was inflated and some were victims who had already been extorted (NCA, 2024b). The extent of subsequent attacks appeared to be exaggerated as well. For example, LockBit claimed to have successfully attacked the U.S. Federal Reserve, but it was later discovered that its attack was against Evolve Bank & Trust (Ikeda, 2024). After LEA action therefore, LockBit seemed to have not been able to act in the capacity that it said it would.

Apart from downplaying challenges, the groups were found to be opportunistic and sometimes embraced them as opportunities. In order to conduct its exit scam, BlackCat put a fake seizure notice on its website and stated, "*We can officially state that we got screwed by the feds*" (Krebs, 2024). It may also be argued that LockBitSupp leveraged NCA's takedown in 2024 for a series of publicity activities afterwards. One of the most significant was their interview on the Click Here podcast where they sought to downplay challenges and publicise the group further (Temple-Raston and Powers, 2024). This demonstrates their willingness to use challenges – e.g., ongoing threats from law enforcement – to their benefits. The groups could be observed acknowledging challenges directly and taking actions to mitigate them as well. An example was when Conti recommended that its employees take a vacation of 2–3 months around the time of the Conti Leaks (CheckPoint, 2022b). And, in how LockBitSupp acknowledged that LockBit's profits would decrease, even if they claimed that this would only be in the short term; the extent of some LEA action could clearly not be completely discounted (Temple-Raston and Powers, 2024).

4.4.4. Group tactics: a large attack before exit

Focusing specifically on group tactics, BlackCat and Conti were each observed conducting a large attack before discontinuing their brand. This was not seen in LockBit which continues to function despite the persistent LEA action against it (NCA, 2024a; 2024b; Poireault, 2024).

In early 2024, a BlackCat affiliate compromised Change Healthcare resulting in nationwide disruptions to the U.S. healthcare system. To reduce the impact of the attack, Change paid a ransom of $22 million; the affiliate, however, was never paid by BlackCat admins (i.e., the core group) (Greig, 2024). The affiliate complained, but this was followed by the core group announcing that it was ceasing its operations and, according to reports, falsely attributing this to the actions of law enforcement (as mentioned in Section 4.4.3). The takedown notice on their website was widely believed to be fake and was instead a copy of the notice that was used by LEA when they acted against the group in December 2023 (Krebs, 2024). This is not the first time a group has shut down its current operation after a large attack. One of its predecessor

operations, DarkSide, was shut down after its attack against Colonial Pipeline in 2021 (Barry, 2024a). This particular case was not an exit scam, but it does show a trend of abandoning brands when it becomes convenient.

In April 2022, Conti conducted a cyber-attack against government and public sector organisations in Costa Rica and demanded a ransom of $10 million that later increased to $20 million (Sangfor, 2022). This ransom was not paid and the group put a stop to its operations as Conti in May 2022. This attack occurred after Conti's statement of support for Russia and the Conti leaks. In the time since then, the group was observed not to have been as successful in its attacks, resulting in the Costa Rica attack – another instance of failure – being an opportunity to shut down a brand that could no longer be relied upon to bring in significant ransom payments (Sangfor, 2022; Warminsky, 2022). This event is another example of a group marking the end of its operations with a big – albeit unsuccessful in this case – attack. It suggests that some may seek to make one last significant profit with their existing ransomware brands before moving on from the operation when its reputation has been tarnished.

LockBit has not followed this trend. Although it has been working with a reduced level of success since its law enforcement takedown, the group has sought to persist rather than abandon the LockBit brand and cease operations. It has even attempted to appear threatening to important organisations such as when it claimed to have breached the US Federal Reserve, as discussed above (Sharma, 2024). As this attack was fabricated and noting LockBit's own inflated victim numbers, it appears that the group is trying to recover its reputation rather than giving up on its brand.

Table 4 shows a summary of some of the key comparisons across the three groups; the full list can be found in Appendix C.

4.5. Nature of ransomware groups

4.5.1. Opportunistic global targeting

The three groups targeted victim organisations around the world and across a wide variety of sectors. Russia, Russian allies and nations from the CIS were the exception to this modus operandi. Despite the groups claiming to have had restrictions regarding the targeting of healthcare and critical infrastructure, these sectors were observed to have been targeted anyway. For example, France's Center Hospitalier Sud Francilien (CHSF) and the UK's Royal Mail by LockBit (eSentire, 2023), Barts Health NHS Trust (UK) and Change Healthcare (US) by BlackCat (SOCRadar, 2022; Greig, 2024), and the Irish Health Service Executive (Ireland) and Bank Indonesia by Conti (Medlock, 2023; eSentire, 2022).

These actions insinuate that the groups, albeit completely different entities, prioritise their financial earnings above all else. This includes above the ethical implications of attacking national critical infrastructure on which lives depend, or how their actions are perceived by others – especially government bodies responsible for tackling the threat of ransomware – because of such attacks. The wide variety in targets also suggests that the specific harms caused by attacks on organisations (Mott et al., 2024) is not as important as acquiring ransoms from whoever will pay. Targeting broadly has therefore, apparently, enabled the groups to maximise their chances of successfully capitalising on attacks.

4.5.2. A focus on brand

Brand appearance was valued in some capacity by each group, though there was more of this visible with Conti and LockBit. As mentioned earlier, the three groups all advertised and promoted their operations on cybercriminal forums. The advertisement and promotion of the different ransomware brands – especially in the case of Conti and LockBit (DiMaggio, 2023b,2023c) – suggests that the groups valued their brands and sought for them to appear appealing and 'credible' to

Table 4
Comparing the ransomware groups and their dynamics.

Topic of comparison (theme)	BlackCat	LockBit	Conti
Improved version development	Development of Sphynx version. Targeted improved speed and stealth in new versions.	Development of several versions: Abcd, LockBit 2.0, LockBit 3.0, LockBit Green, LockBit-NG-Dev. Targeted improved speed and stealth.	Known to test and improve. Targeted improved speed and stealth.
Challenges and retaliatory actions	Suffered law enforcement takedown. Suffered as members/affiliates broke rules. Retaliatory actions taken by group. Reduction in targeting restrictions. Removal of affiliates.	Suffered law enforcement takedown. Suffered as members/affiliates broke rules. Suffered as banned from cybercriminal forums. Retaliatory actions taken by group. Targeting government, non-profit and educational institutions. Removal of affiliates.	Suffered member leak. Suffered as victims leaked group negotiation chats. Retaliatory actions taken by group. Threat to retaliate to actions against Russia. Leaking victim data if negotiation chats are leaked. Removal of affiliates. Fines for underperforming members/affiliates.
Varying responses to the impact of challenges	Some acknowledgement of challenges faced. Downplayed law enforcement action. Opportunistic in using challenges to its benefit.	Some acknowledgement of challenges faced. Downplayed law enforcement action. LockBitSupp blamed self. Exaggerated victims. Opportunistic in using challenges to its benefit.	Acknowledged challenges of leaks.

others.

In addition, LockBit and Conti sought to disparage their competitors in order to prop up their own ransomware brand. This can be seen in LockBit claiming that other ransomware operations were not worthy competitors: "… *I am too strong for my opponents. Previously, the only worthy competitor as I saw it was AlphV/BlackCat. But now they are gone, and so now I don't see a single worthy competitor.*" (Temple-Raston and Powers, 2024). And, in Conti asserting that other groups were inexperienced or scammers (Kovacs, 2022). BlackCat appeared to be less active in this regard and primarily looked to build their brand by promising not to target certain countries and sectors (Abrams, 2023), and by rewarding internal talent (Symantec, 2022).

The responses to certain activities (e.g., brand imposters or members breaking group rules) were another potential indication of efforts to maintain group image and brand. Two instances of such include LockBit's angry statement about reputational damage in response to a threat actor who used a leaked LockBit builder to attack a German hospital (Tologonov and Fokker, 2024) and how it provided a free decrypter to a children's hospital and claimed to expel the affiliate responsible for the attack from the LockBit programme (Wadhwani, 2023). With Conti, this is also apparent in the internal discussions from the Conti Leaks where members complained about reputational damage occurring when a member attacked a hospital (Burgess, 2022a).

The extent to which all groups valued their brand above their ransom payments appears to be limited however. BlackCat, for instance, quickly relaxed its targeting rules after LEA action. Conti attacked organisations in the healthcare sector such as the Ireland Health Service Executive and the New Zealand Health Department (Securin, 2022). LockBit was also involved in attacks against healthcare organisations such as Capital Health and Contra Costa Health Services, and its claimed attack against Ernest Healthcare following its LEA takedown (Harpur, 2024).

Another notable brand-related observation across groups was the fact that they referred to their operations in ways that made them sound as though they were offering professional or reputable services. This could be seen in how BlackCat would offer victims cyber remediation advice after a breach, reports of how breaches were conducted, and recommendations for avoiding future breaches (CISA, 2024a). LockBitSupp referred to LockBit's business model as, "*post-payment penetration testing*" (Temple-Raston and Powers, 2024). Similarly, Conti claimed that it was a company specialising in "*software for pentesters*" when introducing the company to a potential hire (CheckPoint, 2022a). It may be that the groups were trying to appear professional and present as though they were offering a service to victims to seem reputable and worth engaging with. There is the possibility that this façade was meant to appeal to new recruits and employees as well.

These findings suggest that the groups are all comparable and perhaps unsurprisingly primarily value their ransomware brands as dependable operations for affiliates to join and make money with, rather than (ethical) entities who have strict codes of practice. It may also be that the supposed implementation of targeting rules (e.g., not compromising hospitals) is more about reducing the attention received from LEA and governments rather than about appearing to other criminals as a credible ransomware operation.

4.5.3. The role of deception

Unsurprisingly the groups all were found to engage in several deceptive activities. For instance, all were noted to have kept victim data despite receiving ransom payments. An example of this occurring with BlackCat was when the affiliate who had reportedly been cheated out of their share of Change Healthcare's ransom payment made a statement claiming that they still held the data despite the ransom being paid (Krebs, 2024). In LockBit's case, the February 2022 LEA takedown revealed that data had been kept despite claims that this was not the case (NCA, 2024a). We also found numerous articles warning that even if victims paid ransoms, Conti would not necessarily follow through on decrypting or deleting data (Flashpoint, 2022; Coveware, 2020).

It was not only victims that the groups deceived, but sometimes the group's members themselves. In Conti it was revealed that some members were allegedly not even aware that they were working for a ransomware group and instead they were led to believe that they were working for a legitimate company (Flashpoint, 2022). This point, while undoubtedly surprising to find, does correlate somewhat with the "*software for pentesters*" and "*post-payment penetration testing*" framings mentioned above. The BlackCat affiliate that the group excluded from the Change Healthcare ransomware payment stated that the group had lied to them about receiving the funds (Krebs, 2024). Additionally, an affiliate on a cybercrime forum is known to have complained about LockBitSupp for nonpayment (Seals, 2024). LockBitSupp features often in such cases, including them lying about punishments against its

Table 5
Comparing the nature of the ransomware groups.

Topic of comparison (theme)	BlackCat	LockBit	Conti
Value of brand appearance	Advertises and promotes in cybercrime forums. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.	Advertises and promotes in cybercrime forums. Writing competition. Promotional campaigns. Disparagement of other groups. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.	Advertises and promotes in cybercrime forums. Writing competition. Disparagement of other groups. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.
Lies and deception	Lied about deleting data. Lied to members. Lied about following targeting rules.	Lied about deleting data. Lied to members. Lied about following targeting rules.	Lied about deleting data. Lied to members. Lied about following targeting rules.
Political leanings	Targeting aligned with Russian interests.	Targeting aligned with Russian interests. Claims to be apolitical. References to US politics (and support of certain candidates).	Targeting aligned with Russian interests. Statement of support for Russia's invasion of Ukraine. Anti-western statements made.

Table 6
A summarised comparison of the three groups. A ✔ mark is used to indicate whether a point (e.g., "Based in Russia") is relevant to a particular group.

Group Aspect	Theme		BlackCat	LockBit	Conti
Origins	Country	Based in Russia.	✔	✔	✔
	Predecessor operations	Previous operational groups.	✔		✔
Structure	Ransomware-as-a-Service	Main group developed and maintained ransomware and infrastructure for affiliates.	✔	✔	✔
		Affiliates paid in commission.	✔	✔	
		Affiliates paid in wages.			✔
	Vetting and affiliate status	Recruited from cybercrime forums.	✔	✔	✔
		Recruitment from legitimate sources.			✔
		Required vouching of another criminal to join program.			✔
		Used a referral programme.			✔
		Conducted vetting of affiliates.	✔	✔	
		Required affiliates to achieve certain targets to maintain their affiliate status.			✔
		Required payment to join program.		✔	
		Required proof of experience to join program.		✔	
		Offered Affiliate Plus perks.	✔		
	Business-like structure	Organisational structure evident.	✔	✔	✔
		Different teams with varying roles.	✔	✔	✔
		Development teams present.	✔	✔	✔
		Software testing, Management, HR and Admin teams discovered.			✔
		Affiliates are a core part of the business.	✔	✔	✔
	Leadership	Leader identified.		✔	✔
		Leader possesses public-facing and extroverted persona.		✔	
		Leader possesses internally focused persona.			✔
		Multiple managers with significant roles present.			✔
Organisation	Multiple extortion techniques	Practiced multi-level extortion (double)	✔	✔	✔
		Practiced multi-level extortion (triple)	✔	✔	
		Practiced multi-level extortion (quadruple)	✔		
	Advertisement and promotion	Advertisements on legitimate job sites.			✔
		Promotion on underground forums.	✔	✔	✔
		Technical writing contests.		✔	✔
		Disparaged other groups.		✔	✔
		Ran bug bounty programs.		✔	
		Paid people to get group's tattoo.		✔	
		Competitive commission offered to affiliates	✔		
		Benefit of receiving ransom payment directly and then paying main group commission.		✔	
	Appealing and ease of use product	Customisable ransomware.	✔	✔	
		Fast execution.	✔	✔	✔
		Works across multiple platforms.	✔	✔	
		Sold training documents.			✔
		Darknet leak site used.	✔	✔	✔
		Public data leak site used (likely for added pressure).	✔		
		Automated targeting.		✔	
	Cryptocurrency	Ransom payments used cryptocurrencies.	✔	✔	✔
		Bitcoin cryptocurrency preferred.	✔	✔	✔
		Monero cryptocurrency payments accepted.	✔		
		Cryptocurrency scam involvement and interest.			✔
Dynamics	Improved version development	Targeted improved speed and stealth in new versions.	✔	✔	✔
	Challenges and retaliatory actions	Suffered law enforcement takedown.	✔	✔	
		Suffered member leak.			✔
		Suffered as members/affiliates broke rules.	✔	✔	
		Suffered as banned from cybercriminal forums.		✔	
		Retaliatory actions taken by group.	✔	✔	✔
		Reduction in targeting restrictions.	✔		
		Targeting government, non-profit and educational institutions.		✔	
		Leaking victim data if negotiation chats are leaked.			✔
		Threat to retaliate to actions against Russia.			✔
		Removal of affiliates.	✔	✔	✔
		Fines for underperforming members/affiliates.			✔
		Forum complaints.	✔	✔	
	Varying responses to the impact of challenges	Some acknowledgement of challenges faced.	✔	✔	✔
		Downplayed law enforcement action.	✔	✔	
		Opportunistic in using challenges to its benefit.	✔	✔	
		Blamed self for breach group suffered.		✔	
	Large attack before exit	Large attack before exit	✔		✔
	Law enforcement takedown activity	Experienced takedown	✔	✔	
Nature	Opportunistic global targeting	Global targeting	✔	✔	✔
		Wide variety of sectors	✔	✔	✔
		Avoids targeting CIS countries	✔	✔	✔
	Value of brand appearance	Portrays the operation as a professional service.	✔	✔	✔
		Advertises and promotes in cybercrime forums.	✔	✔	✔
		Promotional campaigns.		✔	
		Writing competition.		✔	✔

(*continued on next page*)

Table 6 (*continued*)

Group Aspect	Theme		BlackCat	LockBit	Conti
		Disparagement of other groups.		✔	✔
		Awareness of reputational damage from attacking certain targets.	✔	✔	✔
	Lies and deception	Lied about deleting data.	✔	✔	✔
		Lied to members.	✔	✔	✔
		Lied about following targeting rules.	✔	✔	✔
	Political leanings	Targeting aligned with Russian interests.	✔	✔	✔
		Claims to be apolitical.		✔	
		Statement of support for Russia's invasion of Ukraine.			✔
		References to US politics (and support of certain candidates).		✔	
		Anti-western statements made.			✔

members for breaking targeting rules. For instance, while LockBitSupp claimed to have removed the affiliate responsible for an attack against a children's hospital, the LockBit takedown revealed that the affiliate in fact continued working with the group (NCA, 2024b).

4.5.4. Political leanings

Political leanings and associations appeared to influence the actions and behaviours of many of the groups. As discussed earlier, they deliberately avoided targeting organisations from Russia and the CIS; thereby suggesting – at least in the first instance – an affiliation with Russian political interests. This was directly apparent in how Conti declared its support for Russia's invasion of Ukraine (Vicens, 2022), when BlackCat maintained that CIS countries – i.e., those connected to the former Soviet Union – remained off-limits when announcing a relaxation of its targeting restrictions (Barry, 2024a), and noting that LockBit ransomware would check whether systems were local to CIS countries before executing an attack (Kaspersky, 2024a).

Despite a statement on LockBit's website that they were apolitical and interested only in money, several comments about President Donald Trump were identified, including ones about court cases that may have affected the 2024 US Election and a statement of support for Trump from LockBitSupp (Flashpoint, 2023; Winder, 2024; Cluley, 2024). Anti-western views were identified in statements from Conti members (CheckPoint, 2022a, 2022b) and in Conti's attack against the Costa Rican government it called for the government to be overthrown: "*We are determined to overthrow the government by means of a cyber attack*" (Burgess, 2022b). In the same stream of blog posts, Conti referred to the President Biden Administration as "*US terrorists*", further alluding to its views (Burgess, 2022b). In sum, although the groups may be primarily opportunistic in their targeting, there is arguably a political angle to their actions and beliefs that sometimes affects their behaviours and statements.

Table 5 shows a summary of some of the key comparisons across the three groups; the full list can be found in Appendix C.

To summarise the most salient comparative findings among the three groups, we present Table 6. We have opted for this more visual representation of the qualitative data analysed to provide a concise summary of the key commonalities and differences across groups. This table visual is also structured such that readers can situate our findings within the broader context of group aspects and themes.

5. Discussion

Ransomware continues to be a significant cybersecurity threat facing society and businesses today. This study sought to address the dearth of evidence-based academic research into the perpetrators of ransomware attacks by investigating three of the most prominent ransomware groups from the last five years, Conti, LockBit and BlackCat/ALPHV. We aim for this work to provide new summative insights into origins, structures, dynamics and nature of such groups. Below, we reflect on our findings and how they may be used to inform activities to tackle the threat posed by such groups. We also introduce the beginnings of a new conceptual framework meant to support the understanding and future evaluation of ransomware groups, and discuss the wider implications of our research.

5.1. Group similarities and links to the wider ransomware threat landscape

Focusing first on the insights into groups' origins, structures, dynamics and nature, the three gangs shared a surprising number of similarities. All had Russian origins, operated a ransomware-as-a-service (RaaS) business model, were structured like businesses with a division of labour, utilised multiple levels of extortion, advertised and promoted their services, made use of cryptocurrency, and improved their ransomware strains continuously. They also took retaliatory actions against perceived threats, targeted organisations globally, attacked victims across a wide range of sectors, valued their brand, lied and had some level of political affiliation. Considering these findings in relation to the larger ransomware group ecosystem, there are similarities and differences of note.

Comparable aspects include the dominance of Russian groups in the market (accounting for 69% of all cryptocurrency proceeds linked to ransomware) (Toulas, 2024), and use of RaaS and double extortion techniques (as seen with other groups such as Play/Playcrypt, RansomHub, Hellcat, SafePay) (CISA, 2023c; CISA, 2024b; Coker, 2024; Coker, 2025; Greig, 2025a). Several factors do, however, distinguish these groups and set them apart from their peers. BlackCat and LockBit have, for example, progressed beyond double extortion to more aggressive tactics, and the three groups arguably functioned the most like businesses in their recruitment, promotion and activities; these may also be signs of maturity.

There were numerous similarities emerging between only two of the three groups. For example, BlackCat and LockBit offering their affiliates ransom commission compared to Conti paying affiliates a set wage, Conti and BlackCat being successor operations whereas LockBit was not, and LockBit and BlackCat having suffered a law enforcement takedown whereas Conti did not. Additionally, Conti and BlackCat ceased operations after conducting a large attack following significant challenges for the groups whereas LockBit has instead attempted to persist in its operations since facing the challenge of its own LEA takedown. We also

note the strong leadership personas exhibited in Conti and LockBit, and their significant emphasis on brand through promotions and advertisements. These activities exemplify the range of behaviours also witnessed, in part, across other groups. These span, origins in other groups (e.g., the Akira and Royal groups originating in Conti/Ryuk (Hostetler and Campbell, 2024)) but also new beginnings (e.g., Play and SafePay emerging as new closed groups (CISA, 2023c; Cluley, 2025a)) and potential exit scams (such as those linked to the DarkSide group's actions in 2021 (Cimpanu, 2021)).

It is perhaps unsurprising that groups that have emerged and become prominent around the same general time have been found to share similarities in their nature, structure and dynamics. It suggests that there are multiple aspects of ransomware groups – in those studied and across the threat landscape – that appear to enable them to gain prominence or appear as symptoms of successful operations. These aspects may have been adopted from other prior groups and can also be witnessed in less mature groups presumably to boost their success likelihood. It is prudent to remember the fact that groups often seem to succeed others or poach members from other groups (see Section 4.1.2), and therefore that factor could influence such similarities.

The Russian origins of several ransomware groups suggests that such origins may be characteristic of prominent ransomware operations; one may even conclude that it is advantageous for an operation to originate from that locale. This is a reasonable point considering the historic tensions between Russia and the West (Johansmeyer et al., 2025). As was discussed by Martin and Whelan (2023), affiliation with the Russian state can indicate a level of tacit approval by the state and can serve as a means of protection for ransomware threat actors. This may well be a reason why groups primarily emerge from that area even although there are other countries with capable and willing ransomware threat actors (Unit 42, 2024). With BlackCat, Conti, LockBit and several other groups having Russian ties, cybercriminals often tend to be out of the physical and legal reach of Western law enforcement agencies (i.e., the locations where attacks tended to target). This suggests that efforts may be best dedicated to the disruption of operations and exposure of criminal identities above attempts to directly seize criminals based in Russia.

5.2. Business importance of brand and reputation

Several findings that emerged from our investigation were particularly salient. The critical importance of branding and reputation, for instance. Promotions and other public relation activities to make group operations and their brands attractive to potential collaborators were noteworthy. In particular, we highlight an emphasis on creating appealing products and services, boosting brand appeal via competitions, attempts to look 'ethical' in their targeting, and acting as professional service entities.

Brand is especially important for the RaaS business model as the success of attacks relies on a strong service offered by the main group and a large pool of affiliates to execute the attacks. This may be why the groups appeared to: prioritise the development of quick, effective and easy-to-use tools; enable and support affiliates as much as possible; and disparage the operations of other competing groups. In the wider ransomware ecosystem, we can see similar emphasis placed on brand-building and especially in enabling more effective affiliates. A poignant recent example of this is where the Qilin group added a "Call Lawyer" feature for affiliates with the purpose of providing legal consultation to increase the pressure on victims during ransom negotiations (Tsipershtein and Ananin, 2025).

The significance of brand and reputation also resonates for operations not operating as RaaS. The once closed Play/Playcrypt group presents an example of the importance and use of these aspects. On its 'frequently asked questions' TOR victim page, it responds to the question "*How can i trust you?*" with, "*We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners*" (Imano and Slaughter, 2022). The argument, therefore, is that it pays close attention to maintaining a good reputation and does not leave it to others. Ironically, Play/Playcrypt seems to have now progressed from a closed operation to be sold as a service (Lakshmanan, 2023). This reinforces the perspective that without a good 'product' and a reliable pool of affiliates, the ability for a ransomware operation to grow is limited.

The effect of damage to a ransomware brand can be observed in all three groups. When the groups were hit by large-scale challenges such as the Conti Leaks or law enforcement takedowns, their ability to carry on as normal was severely impacted, resulting in a reduced number of victims, or even the termination of the brand altogether. Conti and BlackCat both ended their operations while LockBit has attempted to continue operations though with a reduced number of victims. This seems to indicate that if a ransomware group faces a large enough incident that damages its reputation (including exposing the identities of central members), the brand may be tarnished, and it can become unappealing for criminal actors to continue to support and work with it. The HIVE, Phobos and 8Base takedowns are further examples of this impact (Department of Justice (DOJ), 2023; Europol, 2025). Efforts to publicly damage the reputation of groups may then be useful at causing members and affiliates lose their faith in brands and cease their collaboration with them.

This is not, of course, a panacea and such efforts require significant amounts of international coordination and resources, as seen with the NCA-led takedown of LockBit which involved the FBI, DOJ, Europol and Australian Federal Police (National Crime Agency (NCA), 2024a; National Crime Agency (NCA), 2024b) and Europol-led takedown of Phobos and 8Base involving an international group of LEAs (Europol, 2025). Furthermore, such action would not necessarily stop new operations from forming as numerous groups have been observed to set up successor operations after discontinuing a brand. It may nonetheless disrupt operations enough or provide a platform for threat actors to be caught. Tracking successor operations could be helpful as well considering that understanding common behaviours and tactics from past operations may aid in anticipating the actions of succeeding operations (Arghire, 2024). Tactics, Techniques and Procedures (TTPs) are likely to align with behaviours from previously observed groups and therefore these can be used to inform cybersecurity policy, especially in cases when an actor is known to be a successor operation.

5.3. Cryptocurrency and multiple extortion as standard

Another observation worth discussion is the central role of cryptocurrency in ransomware operations. This is one of the more studied topics in cybercrime academic research, but its relevance here deserves some mention. Across the three groups, cryptocurrency – particularly Bitcoin – is the standard method for payments. This matches the wider cybercriminal market and prominence of digital currencies (Carlisle, 2023). Research has explored the link between ransomware groups and cryptocurrencies and presented several technical, legal and political reasons why groups rely on them (Katagiri, 2023). Notwithstanding their elusiveness, attempts to combat ransomware groups should

investigate novel ways to trace and block suspicious payments in order to disrupt operations.

Analysing cryptocurrency payments is a fruitful area of practice and research, and has previously been explored with Conti, HIVE, SamSam, Jigsaw and others (Paquet-Clouston et al., 2019; Gray et al., 2022; Chainalysis, 2024a; 2024b; Sophos, 2025). The reliance on cryptocurrency suggests that analysing and tracking payments relating to specific ransomware groups is a worthwhile endeavour in disrupting their activities. A pertinent example of this when the U.S. Department of Justice recovered 63.7 bitcoins ($2.3 million) of the ransom paid to DarkSide after its attack on Colonial Pipeline (DOJ, 2021). Tracking payments has also provided new insights into the significant impact of takedown operations as seen with HIVE, which the FBI estimates prevented approximately U.S. $130 million in ransom payments to the group (Chainalysis, 2024a). If law enforcement, potentially in collaboration with industry (especially companies that specialise in cryptocurrency and blockchain analysis), is better able to analyse and track these payments, they may be able to further thwart ransomware actors.

The increasing aggressiveness of ransomware groups deserves some attention. In our study, the three groups all utilised double extortion and, in some cases, even triple and quadruple extortion. While the latter two types are less common in other groups, the drive for making profits in an increasingly competitive market may lead groups to more hostile tactics. Such tactics are likely to be informed by what are the easiest actions to perform and what is likely to be the most successful, including actions that would damage an organisation's reputation with customers, suppliers, or regulators.

A recent example of this can be seen with Hellcat, another quickly rising group, that used psychological humiliation tactics – e.g., requesting a $125,000 payment from a French company in baguettes – to gain publicity and further pressure companies into paying (Coker, 2025). In the case of another new group, i.e., AiLock, it has directly threatened to inform regulators and a company's competitors of the breach. Their ransom note reads: "*All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company's customers will be published on the internet, and the respective country's personal data usage authority will be informed*" (Cluley, 2025b). Given these findings and developments generally, this suggests that at the least, organisations should anticipate ransomware attacks will consist of both the exfiltration and encryption of data; regardless of what the threat actor claims.

Efforts should be taken to prioritise prevention and quick detection of attacks in the first place where possible, considering that while backups may resolve the issue of encryption (albeit not perfectly (Ro, 2024; National Cyber Security Centre (NCSC), 2024)) they will not help in the case of exfiltrated data being leaked. Additionally, the threat of further layers of extortion such as threats to DDoS and threats to attack partner organisations suggests that DDoS countermeasures should be taken. Organisations should also comprehensively consider vulnerabilities in partners or their supply chain when implementing cybersecurity policies to reduce the likelihood that potential weak points in partners are leveraged by ransomware groups. There have been various instances of debilitating ransomware attacks (and attempted attacks) involving third parties over the last five years including the 2025 attacks on Marks and Spencer and The Co-Op (Abrams, 2025; Cyber Monitoring Centre, 2025; Edwards, 2025) and the 2023 attack on the British Library (The British Library, 2024).

5.4. Towards a conceptual framework to understand ransomware groups

In addition to providing evidence-based comparative insights across three of the most prominent ransomware groups to date, this research also pursued an important secondary goal: contributing to the more theoretical and foundational study of ransomware groups more broadly. As discussed in Section 2, there is a notable lack of academic research

Table 7
A conceptual framework for understanding ransomware groups.

Group area	Characteristic	Key questions
Origins	Country of origin or affiliation	What country(ies) is the group based in or strongly affiliated with?
	First known activity	When did the group first become active? What was the nature of their earliest observed operations?
	Predecessor or linked operations	Which prior cybercriminal or ransomware groups are connected to this group?
Structure	Business model (e.g., Ransomware-as-a-Service)	Does the group operate a Ransomware-as-a-Service (RaaS) model? If so, how are affiliates compensated (e.g., fixed wage, commission from core group, or self-managed)? If not, what alternative model is used?
	Affiliate recruitment, vetting, and status	How are affiliates recruited and vetted? What criteria determine changes in their status (e.g., promotion, expulsion)? Are there formal or informal rules governing affiliate conduct?
	Business-like structure (or other structure)	Does the group exhibit a business-like structure? If so, what roles or divisions exist within it, and how are responsibilities allocated? If not, how is it structured?
	Leadership profiles	Are any group leaders publicly known or identifiable? What is known about their roles, visibility, or personas (e.g., public-facing, anonymous, or operational only)?
Organisation	Advertisement and promotion activities	How and where does the group promote itself? Are advertisements shared on dark web forums, or other channels?
	Ransomware features and differentiation (e.g., appeal and ease of use)	How does the group differentiate its ransomware strains (e.g., usability, technical sophistication, effectiveness)? What features are emphasised to appeal to affiliates or other users?
	Extortion techniques	What extortion methods are used by the group? Are multiple extortion techniques common, if so, which ones?
	Cryptocurrency usage	Are cryptocurrencies used for ransom payments? If so, which ones? Do they serve other purposes within the group's operations (e.g., payments to affiliates, scams)?
Dynamics	Version development and improvements	How actively does the group develop or update its ransomware strains? What versions or variants exist, and how have they evolved over time?
	Law enforcement takedown	Has the group been subject to law enforcement action? If so, when did it occur, and what were the outcomes or consequences for the group's operations?
	Challenges faced and retaliatory actions	What challenges has the group encountered generally (from internal or external sources)? What retaliatory actions has the group engaged in, against whom, and in what challenging situations?
	Public response to challenges	How has the group publicly responded to any significant disruptions (e.g., law enforcement operations, leaks, affiliate disputes)? If it has responded, has it sought to downplay or capitalise on these challenges?

(*continued on next page*)

Table 7 (*continued*)

Group area	Characteristic	Key questions
	Brand longevity	Is the group or its brand still active? If not, when did it become inactive?
	Exit attacks	If the group ceased operations, did it conduct a final large-scale attack before exiting? If so, how did they conduct the attack and eventually exit (cease their brand)?
Nature	Country targeting	Which countries or regions does the group typically target? Are there any notable exclusions or avoidance patterns?
	Brand portrayal and value	How does the group present or promote its brand publicly and within cybercrime forums or marketplaces? What image or reputation does it aim to project? Does that image have undertones of legitimacy?
	Use of lies and deception	To what extent does the group rely on deception in its operations or messaging (e.g., false claims, impersonation, misinformation)
	Political affiliations or leanings	Does the group express or imply any political motivations, ideologies, or nation-state affiliations?

examining the internal, social components of ransomware groups. This gap presents an opportunity to develop mechanisms, such as conceptual frameworks, that facilitate a deeper understanding of these groups, including the ability to characterise and compare them. Such a framework could be highly valuable to researchers and practitioners in law enforcement, cybersecurity, and policymaking. It would support activities such as more targeted research, standardised group profiling, tracking of related, predecessor or successor groups, and, ultimately, disruption based on the insights gained (Turvey, 2011).

There are several approaches through which such frameworks or models can be constructed. For instance, Ahmad et al. (2012) drew on existing literature and Grounded Theory to develop a conceptual framework for understanding cyber terrorism, highlighting the value of literature in generating new knowledge. Similarly, Agrafiotis et al. (2018) used qualitative content analysis of news articles, academic literature, and cyber-incident databases to extract relevant harms and their relationships, thereby developing their cyber harm model; notably, they also use inductive and deductive approaches. Other studies that combine literature and qualitative analysis to construct conceptual models include Sergi and Storti (2021) and Paarlberg (2022). Together, these works offer a strong precedent on which we base our own framework.

To define our framework, we drew inspiration from the aforementioned prior research and leveraged the thematic analysis process and results (i.e., themes and areas) that emerged from our primary study. This allowed us to build on the rigorous methodological approach outlined in Section 3 and extend it to the development of a conceptual framework. Using these high-level themes also reflects good practice in qualitative analysis, as it enables future researchers to adapt and build upon existing research artefacts rather than replicate the analysis from scratch (Ritchie et al., 2022). The resulting conceptual framework is presented in Table 7.

As shown, the framework is closely aligned with the analyses in Section 4 and the comparative table in Appendix C. It centres on the five core areas of a ransomware group (namely, origins, structure, organisation, dynamics, and nature) and defines specific characteristics (formerly themes) to be collected about the group under study. To enhance usability, the wording of certain characteristics has been refined (e.g., "Country based in" becomes "Country of origin or affiliation"), and the framework includes sample questions to guide users. For example, when assessing affiliates, one might ask: How are affiliates recruited and vetted? What criteria determine changes in their status (e.g., promotion, expulsion)? This list of questions is not exhaustive and may be adapted by users depending on their context and data access. For instance, law enforcement agencies may have more detailed data than academic researchers and could therefore include more probing questions.

Once data is collected using this framework, it can be updated over time to build a comprehensive profile and knowledge base on the group. Most importantly, it can also serve as the foundation for comparative analyses across multiple groups, as demonstrated in this article's research. Ultimately, we see these as essential activities for advancing the study, and enabling the disruption, of the ransomware ecosystem.

5.5. Theoretical and practical implications

This research offers several theoretical and practical implications for the study and analysis of ransomware groups.

5.5.1. Theoretical implications

Focusing first on theory, our findings demonstrate clear patterns and recurring themes across the ransomware groups examined. Two significant points emerge that we believe warrant particular attention from the academic community.

First, our analysis reveals that reputation and brand capital are critical resources within the cybercriminal ecosystem. While this supports broader research on cybercrime (Décary-Hétu and Dupont, 2013), our findings suggest that these factors play an even more central role in the ransomware landscape. We consistently observed how brand influenced group recruitment, status, retaliatory actions, and longevity. Although the importance of brand and reputation has been acknowledged in general cybercrime literature, academic research specifically addressing this dynamic within ransomware groups remains limited. Given its prominence, this appears to be a valuable area for further investigation. Second, our research highlights the organisational maturity achieved by leading ransomware groups. We identified hierarchical structures, specialised teams, and administrative roles that closely resemble those of corporate entities. This represents a shift from earlier academic conceptualisations of ransomware groups, which often overlooked such levels of organisation. Only recently has academic work begun to acknowledge the complex internal structures of these groups (Whelan et al., 2024). Viewing these actors as organised enterprises may provide novel insights into their operations and potential disruption strategies (Leukfeldt et al., 2017). These two points are further developed later in this section, where we present actionable recommendations to address the threat of ransomware.

A further theoretical contribution is the conceptual framework introduced in Section 5.4, which provides a structured approach for

understanding ransomware groups. By leveraging our primary analysis, this framework provides a platform to enable future researchers to examine and compare the origins, structure, organisation, dynamics and nature of other ransomware groups. It can serve both as a reference for validating future findings and as a foundation for studying the growing number of ransomware organisations. Importantly, this framework also has practical utility for law enforcement, cybersecurity professionals, and policymakers as discussed next.

5.5.2. Practical implications and actionable recommendations

Our research yields several direct practical implications. One actionable recommendation involves leveraging the importance of branding and reputation to undermine ransomware groups. As hinted at in Section 5.2, publicly damaging a group's reputation may erode internal confidence and discourage collaboration. We advocate for actions such as amplifying a group's operational failures (such as technical errors in file decryption despite ransom payment as happened with Ryuk (Emisoft, 2019), or unsuccessful responses to law enforcement action) as this could reduce its standing among members, affiliates, and potential victims (considering payment).

Another strategy involves publishing or leaking sensitive information, such as details of group members, internal conflicts, or scams targeting affiliates, on cybercriminal forums where the group is active. The NCA's recent takedown of LockBit offers early examples of such tactics (NCA, 2024a; NCA, 2024b). These interventions may also destabilise leadership structures, which can also be a useful strategy at disruption (Ficara et al., 2023). A more contentious approach involves the use of misinformation. This should, however, be properly deliberated because it is ethically debatable whether planting false information is a justified pre-emptive strategy. Hypothetical examples include suggesting that a group's leadership is cooperating with law enforcement or that internal betrayal (via gathering and public leakage of chat logs and internal data) is imminent. Such strategies resonate with broader concepts from cyber deception research, which explores misleading attackers to aid in defence (Wang and Lu, 2018).

Another important theme from our findings is the continuous rise of the RaaS model. This featured prominently in each of the groups studied and now appears to be a standard progression even if a group begins as closed (as we discussed earlier with Play/Playcrypt (Lakshmanan, 2023)). The prominence of affiliates presents multiple points of potential intervention. We advocate for several activities to be considered: the infiltration and exploitation of cybercriminal forums where affiliates are recruited (this could disrupt the critical affiliate recruitment and vetting process we highlighted); targeted operations and strong legal action against affiliates (affiliates may be more geographically and legally accessible than core members – as seen in Greig (2025b)); incentivising affiliate defection (this could enable infiltration and intelligence gathering); and seeding rivalry between groups (for example, seeding claims that a group is actively stealing poaching affiliates, with the aim of sparking conflict).

Our research and prior work also underscore that many ransomware groups are based in Russia, which often limits the feasibility of arrests. Consequently, efforts may be better focused on operational disruption and public exposure of group members. Recent actions such as the NCA-led Operation Cronos targeting LockBit (NCA, 2024a; NCA, 2024b) and the FBI's takedown of the HIVE group (DOJ, 2023) illustrate this approach. Where group members operate outside Russia, arrests are not only possible but increasingly frequent (Tidy, 2023; Reddick, 2024; DOJ, 2024; Europol, 2025). Furthermore, cross-sector and international collaboration is essential. Enhanced intelligence sharing can strengthen defences against ransomware threats. The Counter Ransomware Initiative (Counter Ransomware Initiative (CRI), 2023) is an early example of this kind of cooperation. Defensive strategies should also recognise that no organisation, with the apparent exception of those in the CIS region (assuming Russian-affiliated groups), is truly off-limits, and that targeting may be aligned with Russian political interests.

Finally, organisations must prepare for increasingly sophisticated and layered extortion attempts. Ransomware actors are opportunistic and adaptable, often combining multiple tactics such as: full data/system encryption; data exfiltration and threats of public leakage; direct communication with third parties affected by the breach; and reporting victims to regulatory authorities (e.g., the SEC). Preparation should focus on reducing the impact and harms of these actions. Existing research into the harms from ransomware attacks (e.g., Mott et al., 2024; Pattnaik et al., 2023) may also be helpful at aiding organisation in scoping the ways in which they may be impacted. At a minimum, organisations should strengthen internal controls, such as data segmentation and encryption, to mitigate the consequences of a successful attack.

5.6. Limitations and future work

There are limitations of this research which should be acknowledged. The most prominent stems from the nature of the study and its focus on cybercriminal groups. Such groups are intentionally elusive, prioritise anonymity, and operate in underground and secret spaces. These factors make it difficult to find complete and reliable information on the groups thereby impacting any research exploring their origins, structure, organisation, dynamic or nature. We sought to mitigate the impact of this limitation by examining numerous sources and triangulating the data gathered for our research; this also involved focusing on more up-to-date sources of information. These actions further helped to mitigate another limitation, i.e., relying on inaccurate sources, misinformation or propaganda. By focusing on corroborated, updated sources and those that were from official entities (e.g., CISA, NCSC, DOJ) and industry-based research studies (e.g., CheckPoint (2022a; 2022b), Krebs (2022), TrendMicro (2024)), we were able to increase the reliability of our findings. Nonetheless, given the points above this is a limitation that should be noted.

Another limitation to this study links to use of Google Search. While Google was specifically selected because of its prominence and coverage of sources,[1] their algorithms are proprietary and largely unknown to the public. It is possible therefore that search results may differ across readers and potentially change over time. We attempted to mitigate the significance of this risk during the search process by not logging in to an account, using anonymous browsing, and completing the search over a month. This point is still, however, an important one which we acknowledge may impact the reproducibility of the results.

Considering our concentration and comparison of three groups, we also acknowledge that the amount of information available on the characteristics of each group was not equal. As such, this could have impacted the quality of the comparisons made. For example, there is more known publicly about the structure of Conti than of BlackCat because of the Conti leaks; BlackCat has not experienced an equivalent-sized leak. Similarly, LockBit's leader is more extroverted and vocal, and therefore more is understood about the leadership of LockBit than of other groups. We expect that as law enforcement takedown operations increase, more information will become available on groups that could be used for future analysis.

There are several potential avenues for further research; much of which could build on the findings from our work. The first relates to expanding this study to incorporate analyses and comparisons to other prominent, but less mature ransomware groups. This could also leverage the conceptual framework and the data gathered in Appendix C. Such comparisons may be helpful at identifying ways to predict group changes or assist in disruption actions targeting newer groups. Examples of groups that are quickly growing in notoriety include SafePay, Bert,

[1] "The Google Search index covers hundreds of billions of webpages and is well over 100,000,000 gigabytes in size." https://www.google.com/intl/en_us/search/howsearchworks/how-search-works/organizing-information/

FunkSec, Ailock and Anubis, for instance. If research is able to detect notable similarities, it may provide the platform for better mitigation. An important, related factor is data, and access to data on these (and other) groups. In our research, we leveraged openly-sourced data including datasets from significant leaks. Another way to gather data – which could be pursued by future work – is by active monitoring, for instance, joining criminal forums or dark web groups directly. This would provide direct access which could lead to more novel, empirical insights. However, there are several safety, ethical and legal risks that would first need to be assessed and balanced against the value from this endeavour (Thomas et al., 2017).

Future studies may also benefit from conducting reviews with a narrower focus. The present study included a comparative thematic review of five areas of three ransomware groups. Although our analysis was able to cover a substantial amount of content, a narrower focus in subsequent work could allow for more detailed assessment of individual areas of interest (e.g., only the group's organisation or structure). This current research, including the conceptual framework, would provide a basis for such future work. Another important point is that different themes may be identified in groups outside of those selected for the present study (i.e., those in Appendix B) and future ransomware groups may have separate themes of their own. Furthermore, ransomware may adapt or change in ways not currently envisaged. It would therefore be beneficial to periodically conduct similar future research into upcoming groups to identify changes in characteristics/themes over time that may offer further insight into how ransomware groups change and how they can be better disrupted and their impacts mitigated. Such changes could also be used to refine or adapt the conceptual framework to enable its continued usage.

6. Conclusion

This study has advanced academic research on the topic of ransomware by investigating the origins, structure, organisation, dynamics and nature of an exemplar of three prolific ransomware groups, BlackCat/ALPHV, Conti and LockBit. The novelty of our research stems from its systematic collection and analysis of fragmented and dispersed data on these prominent groups and the extraction of insights relevant to the academic security research community. We were also able to leverage learnings from that analysis to introduce a new conceptual framework through which ransomware groups could be studied in the future.

Reflecting on our primary contribution's findings, overall, we found that the groups shared many similarities such as their Russian origins, global targeting, use of a ransomware-as-a-service structure, their valuing of their brand and their common use of cryptocurrency and multiple levels of extortion. These similarities are useful for informing the approaches that organisations and law enforcement take in regard to the threat of ransomware groups. An especially noteworthy finding was the role and value of a ransomware group's brand in its operation. It was posited that damaging the reputation of a ransomware group could restrict its effectiveness and lead to groups either having to reorganise under a new brand or otherwise attempt to persist but potentially with less success. This strategy may be particularly useful when the geographic locations or origins of a group make the arrest and prosecution of its members difficult.

Despite the benefits of damaging the reputation of ransomware group brands, attention should still be placed on measures to prevent ransomware attacks from occurring in the first place. This is due to the standard practices that the groups use such as double extortion which can create challenges for victims even if they can restore systems from regular backups. Additionally, as groups with damaged brands are known to regroup under new names and operations, disruption of ransomware groups may only have a temporary benefit of slowing down operations rather than stopping them for good and in the long term. Since disbanding, Conti is known to have had its members split off into smaller groups (Ikeda, 2022; Kovacs, 2022) and a recent article suggests that a new ransomware group known as "Cicada3301" may be a successor group to BlackCat as it shares many similarities with them (Muncaster, 2024). This suggests that the trend of new brands succeeding old ones with damaged reputations will continue and therefore it is important to be aware of this when considering the threats they pose and how to deal with them.

CRediT authorship contribution statement

Andrew Phipps: Writing – review & editing, Writing – original draft, Methodology, Investigation, Data curation, Conceptualization. **Jason R. C. Nurse:** Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Validation, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Search terms

Conti:

Conti ransomware AND (Origins OR Structure OR Organisation OR Dynamics OR Nature OR Character OR Affiliate OR Business OR Recruitment OR Profile OR Reputation OR Branding OR Employee OR Disruption OR Attack OR Target OR Victim OR Developer OR Extortion OR Takedown OR Salary OR Research OR Boss OR Country OR Activities OR Leak)

LockBit:

LockBit OR "Lock Bit" OR abcd ransomware AND (Origins OR Structure OR Organisation OR Dynamics OR Nature OR Character OR Affiliate OR Business OR Recruitment OR Profile OR Reputation OR Branding OR Employee OR Disruption OR Attack OR Target OR Victim OR Developer OR Extortion OR Takedown OR Salary OR Research OR Boss OR Country OR Activities OR Leak)

BlackCat/ALPHV/Noberus:

BlackCat OR "Black Cat" OR ALPHV OR Noberus ransomware AND (Origins OR Structure OR Organisation OR Dynamics OR Nature OR Character OR Affiliate OR Business OR Recruitment OR Profile OR Reputation OR Branding OR Employee OR Disruption OR Attack OR Target OR Victim OR Developer OR Extortion OR Takedown OR Salary OR Research OR Boss OR Country OR Activities OR Leak)

Appendix B. PRISMA Flow Diagram

Fig. B1.

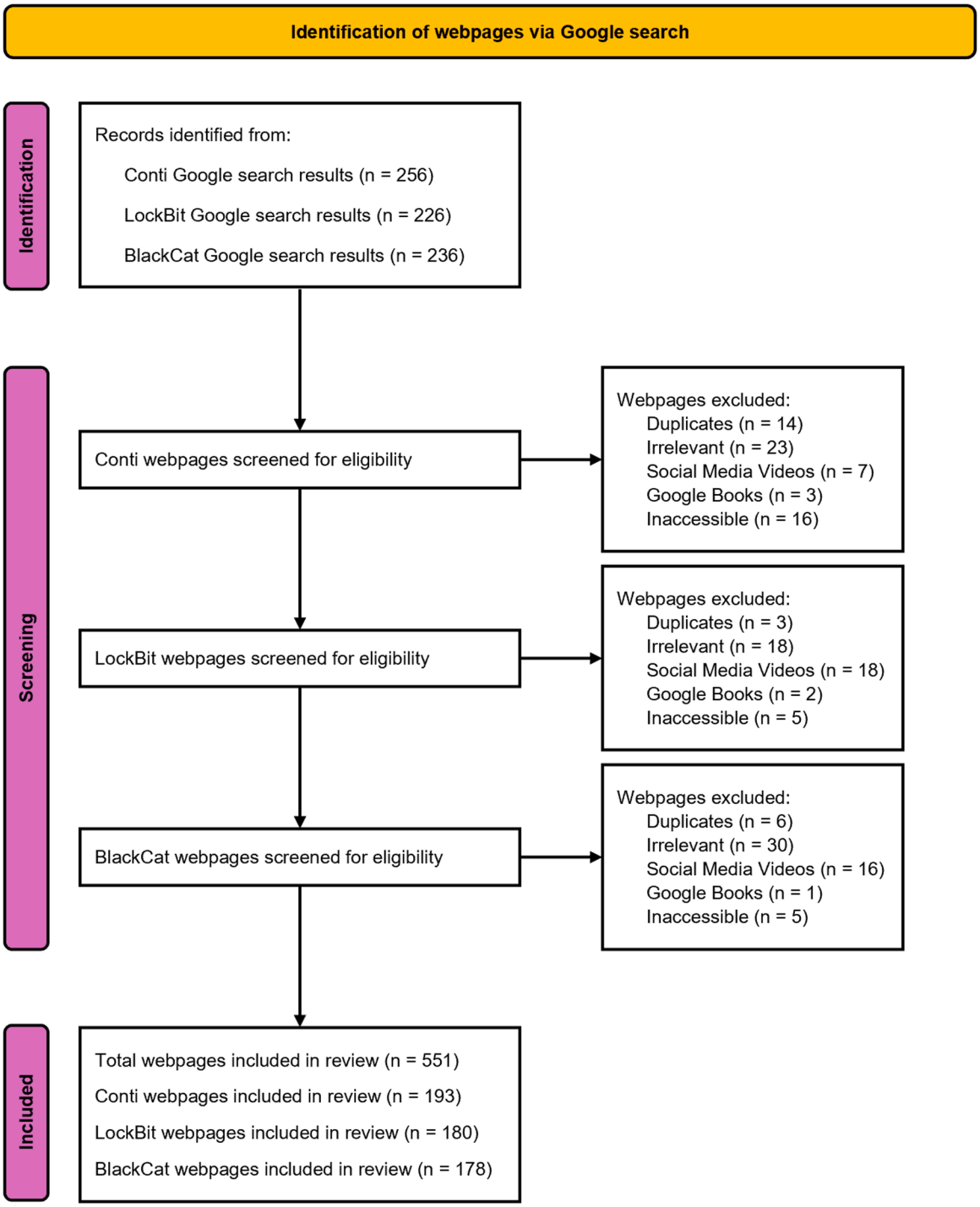

Fig. B1. PRISMA flow diagram for the study conducted.

Appendix C: Comparative table

This presents a comparative table of the groups under study.

Group Aspect	Theme	BlackCat	LockBit	Conti
Origins	Country based in	Russia	Russia	Russia
	First appearance	November 2021	September 2019 (abcd)	2019
	Predecessor operations	DarkSide, Blackmatter, REvil	N/A	Ryuk, TrickBot, Emotet
Structure	Ransomware-as-a-Service	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates are paid up to 90 % commission.	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates receive ransom and pay main group 20 % commission.	Main group developed and maintained ransomware and infrastructure for affiliates. Affiliates paid a set wage.
	Vetting and affiliate status	Recruited from cybercrime forums. Conducted vetting of affiliates. Required affiliates to achieve certain targets to maintain their affiliate status. Offered Affiliate Plus perks.	Recruited from cybercrime forums. Conducted vetting of affiliates. Required payment to join program. Required affiliates to achieve certain targets to maintain their affiliate status. Required proof of experience to join program.	Recruited from cybercrime forums. Recruitment from legitimate sources. Required vouching of another criminal to join program. Used a referral programme. Required affiliates to achieve certain targets to maintain their affiliate status.
	Business-like structure	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business.	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business.	Organisational structure evident. Different teams with varying roles. Development teams present. Affiliates are a core part of the business. Software testing, Management, HR and Admin teams discovered.
	Leadership	No specific leading member identified.	LockBitSupp identified as leader. Public-facing and extroverted persona.	Stern identified as leader. Internally focused persona. Multiple managers with significant roles.
Organisation	Multiple extortion techniques	Practiced multi-level extortion: Double, triple, quadruple. Activities discovered: Encryption, Exfiltration, DDoS, Associate targeting, Reporting victim breach.	Practiced multi-level extortion: Double, triple. Activities discovered: Encryption, Exfiltration, DDoS.	Practiced multi-level extortion: Double. Activities discovered: Encryption, Exfiltration.
	Advertisement and promotion	Promotion on underground forums. Competitive commission offered (90 %).	Promotion on underground forums. Technical writing contests. Paid people to get LockBit tattoo. Ran bug bounty programs. Offered of reward to anyone who could uncover LockBitSupp's identity. Disparaged other groups. Benefit of receiving ransom payment directly and then paying main group commission. Sought to be appealing with the aim of recruiting affiliates from other groups.	Promotion on underground forums. Technical writing contests. Disparagement of other groups. Advertisements on legitimate job sites.
	Appealing and ease of use product	Highly customisable ransomware. Fast execution. Works across multiple platforms: Windows, Linux. Rust programming language used. Darknet leak site used. Public data leak site used (likely for added pressure). Leaked data search.	Customisable ransomware. Fast execution. Availability of a custom exfiltration tool (StealBit). Works across multiple platforms: Windows, Linux, MacOS. Darknet leak site used. Automated targeting.	Fast execution. Darknet leak site used. Works primarily on Windows. Sold training documents.
	Cryptocurrency	Ransom payments used cryptocurrencies. Bitcoin cryptocurrency preferred. Monero cryptocurrency payments accepted and could result in a discount for victims.	Ransom payments used cryptocurrencies. Bitcoin cryptocurrency preferred.	Ransom payments used cryptocurrencies. Bitcoin cryptocurrency preferred. Cryptocurrency scam involvement and interest.
Dynamics	Improved version development	Development of Sphynx version. Targeted improved speed and stealth in new versions.	Development of several versions: Abcd, LockBit 2.0, LockBit 3.0, LockBit Green, LockBit-NG-Dev. Targeted improved speed and stealth in new versions.	Known to test and improve. Targeted improved speed and stealth in new versions.
	Challenges and retaliatory actions	Suffered law enforcement takedown. Suffered as members/affiliates broke rules. Retaliatory actions taken by group. Reduction in targeting restrictions. Removal of affiliates. Forum complaints.	Suffered law enforcement takedown. Suffered as members/affiliates broke rules. Suffered as banned from cybercriminal forums. Retaliatory actions taken by group. Targeting government, non-profit and educational institutions. Removal of affiliates. Forum complaints.	Suffered member leak. Suffered as victims leaked group negotiation chats. Retaliatory actions taken by group. Threat to retaliate to actions against Russia. Leaking victim data if negotiation chats are leaked. Removal of affiliates.

(*continued on next page*)

(*continued*)

				Fines for underperforming members/ affiliates.
	Varying responses to the impact of challenges	Some acknowledgement of challenges faced. Downplayed law enforcement action. Opportunistic in using challenges to its benefit.	Some acknowledgement of challenges faced. Downplayed law enforcement action. LockBitSupp blamed self for breach group suffered. Exaggerated victim numbers. Opportunistic in using challenges to its benefit.	Acknowledged challenges of related to Conti leaks.
	Large attack before exit	Conducted an exit scam after the Change Healthcare attack (February-March 2024).	N/A (group has not exited).	Conducted an attack on the Costa Rican Government, and subsequently disbanded (April-May 2022).
	Law enforcement takedown activity	Takedown by the Department of Justice and the FBI in December 2023.	Takedown by the National Crime Agency in February 2024.	N/A
	Operational status	Disbanded/shutdown in March 2024.	Reduced capacity.	Disbanded/shutdown in May 2022.
Nature	Opportunistic global targeting	Global targeting. Wide variety of sectors. Avoids targeting CIS countries	Global targeting. Wide variety of sectors. Avoids targeting CIS countries	Global targeting. Wide variety of sectors. Avoids targeting CIS countries
	Value of brand appearance	Advertises and promotes in cybercrime forums. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.	Advertises and promotes in cybercrime forums. Writing competition. Promotional campaigns. Disparagement of other groups. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.	Advertises and promotes in cybercrime forums. Writing competition. Disparagement of other groups. Awareness of reputational damage from attacking certain targets. Portrays the operation as a professional service.
	Lies and deception	Lied about deleting data. Lied to members. Lied about following targeting rules.	Lied about deleting data. Lied to members. Lied about following targeting rules.	Lied about deleting data. Lied to members. Lied about following targeting rules.
	Political leanings	Targeting aligned with Russian interests.	Targeting aligned with Russian interests. Claims to be apolitical. References to US politics (and support of certain candidates).	Targeting aligned with Russian interests. Statement of support for Russia's invasion of Ukraine. Anti-western statements made.

Appendix D. Summarised group profiles

Conti Ransomware Group Profile

Name: Conti

First appearance: 2019

Country based in: Russia

Predecessor and connected operations: Ryuk, TrickBot, Emotet.

Impacted sectors: Targeting across sectors including: Manufacturing, Government, Healthcare, Retail, Transport, Financial services, Education, Insurance, Critical infrastructure.

Impacted countries: Global targeting including: United States of America, Costa Rica, the Netherlands, Ireland, Switzerland, Japan, France, India, United Kingdom.

Noteworthy attacks: Irish Health Service Executive (2021), Costa Rican Government (2022), Advantech (2020), Broward County Schools (2021), JVCKenwood (2021)

Noteworthy challenges: Leaked affiliate training documents (2021), Public association with Russian government (2022), Conti Leaks (2022).

Motivation: Primarily financial, Possible Russian government association

Extortion Techniques: Exfiltrates data, Encrypts data.

Current Status: Brand has ceased operations in May 2022 following an attack against the Costa Rican government. Members now operate as part of a network of other smaller independent groups such as Black Basta and HIVE.

Overview: Conti is a ransomware group that operates using a ransomware-as-a-service business model. There is a division of labour between members of the group, meaning that some members work on developing and updating the ransomware infrastructure while affiliates of the group gain access to the systems of victims and deploy the ransomware.

The group recruits from both cybercrime forums and legitimate Russian jobhunting sites.

Affiliates are paid a set wage and are relied on to deploy ransomware against victims.

The group is known to be structured like a business with different roles and teams. These include a CEO, managers, developers, HR, testing and admin.

The group first emerged between 2019 and 2020, and its operation is believed to be a successor to Ryuk ransomware and to be closely associated with the actors of TrickBot and Emotet.

The group is primarily based in Russia and consists of Russian-speaking members. It generally avoids targeting countries within the Commonwealth of Independent States.

The group operates a darknet site which it posts data it has exfiltrated from if victims do not pay a ransom.

Following a declaration of support for Russia's invasion of Ukraine, an insider in the group leaked data from Conti such as its internal communications and source code. Due to these leaks and its announced support of the Russian government, which was being sanctioned, the group began to operate only with limited success and ceased operations after a final attack against the Costa Rican government. Members are believed to have split off

into other smaller ransomware groups such as BlackBasta.

LockBit Ransomware Group Profile

Name: LockBit/abcd

First appearance: September 2019

Country based in: Russia

Impacted sectors: Targeting across sectors including: Manufacturing, Critical infrastructure, Education, Healthcare, Financial services, Transportation, Food, Retail, Government, Energy, IT

Impacted countries: Global targeting including: United States of America, United Kingdom, France, Australia, Canada, the Netherlands, Germany, Japan, China, India, Brazil, France, Mexico

Noteworthy attacks: Royal Mail (2023), Accenture (2021), Industrial and Commercial Bank of China (2023), Evolve Bank and Trust (2024), Pendragon (2022), Zaun (2023), Ernest Health (2024), SickKids (2022)

Noteworthy challenges: Leaked ransomware builder (2022), cybercrime forum bans (2024), February law enforcement takedown (2024).

Motivation: Primarily financial. Attacks may align with Russian political interests.

Extortion Techniques: Exfiltrates data, Encrypts data, Threat to DDoS.

Current Status: Brand is continuing operations but with a reduced number of victims following a law enforcement takedown in February 2024. Many affiliates are believed to have moved on to other ransomware-as-a-service operations such as RansomHub.

Overview: LockBit is a ransomware group that operates using a ransomware-as-a-service business model. There is a division of labour between members of the group, meaning that some members work on developing and updating the ransomware infrastructure while affiliates of the group gain access to the systems of victims and deploy the ransomware.

The group recruits from and advertises its services on cybercrime forums. It also runs promotional campaigns.

Affiliates are relied on to deploy ransomware against victims. They receive ransom payments directly and pay a 20 % commission to the main group.

The group is known to be structured like a business and is known to have developers who work on improvements to the ransomware and its infrastructure. The group is led by a persona known as “LockBitSupp”, who was later revealed to be Russian national Dmitry Yuryevich Khoroshev.

The group first emerged in September 2019 as abcd ransomware and became known as LockBit in 2020. Improved versions such as LockBit 2.0, LockBit 3.0 and LockBit Green were released over time.

The group is primarily based in Russia and consists of Russian-speaking members. It generally avoids targeting countries within the Commonwealth of Independent States.

The group operates a darknet site which it posts data it has exfiltrated from if victims do not pay a ransom.

Following a law enforcement takedown in February 2024, there has been a decline in the number of victims that the group has been able to extort, likely due to a loss of trust in the brand. LockBitSupp claims that the brand will persist, but it is believed that many affiliates have moved on to other ransomware-as-a-service operations such as RansomHub.

BlackCat Ransomware Group Profile

Name: BlackCat/ALPHV/Noberus

First appearance: November 2021

Country based in: Russia

Predecessor and connected operations: DarkSide, BlackMatter, REvil

Impacted sectors: Targeting across sectors including: Manufacturing, Financial services, Healthcare, Legal services, IT, Energy, Education, Retail, Government,

Impacted countries: Global targeting including: United States of America, United Kingdom, Australia, India, Canada, Brazil, Taiwan, Spain, France, Japan, the Netherlands, Germany, Italy

Noteworthy attacks: Change Healthcare (2022), Reddit (2023), Tipalti (2023), MGM Resorts (2023), Roblox (2022), MeridianLink (2023), Twitch (2023), HWL Ebsworth (2023), Barts Health NHS Trust (2023), Seiko (2023)

Noteworthy challenges: December 2023 law enforcement takedown (2023), Change Healthcare exit scam (2024)

Motivation: Primarily financial. Attacks may align with Russian political interests.

Extortion Techniques: Exfiltrates data, Encrypts data, Threat to DDoS, Threat to attack associates of victim organisations, Threat to report victim data breach.

Current Status: Brand has ceased operations following an exit scam after an attack against Change Healthcare, resulting in an affiliate not receiving their share of the ransom payment. Many affiliates are believed to have moved on to other ransomware-as-a-service operations.

Overview: BlackCat is a ransomware group that operates using a ransomware-as-a-service business model. There is a division of labour between members of the group, meaning that some members work on developing and updating the ransomware infrastructure while affiliates of the group gain access to the systems of victims and deploy the ransomware.

The group recruits from and advertises its services on cybercrime forums. Affiliates are relied on to deploy ransomware against victims. They are known to receive a commission of up to 90 % of ransom payments.

The group is primarily based in Russia and consists of Russian-speaking members. It generally avoids targeting countries within the Commonwealth of Independent States.

The group is known to be structured like a business and is known to have developers who work on improvements to the ransomware and its infrastructure. The group first emerged in 2021 as ALPHV/BlackCat but this is known to be a rebranding of DarkSide and BlackMatter with members from REvil. The group rebranded from DarkSide after its attack against the Colonial Pipeline.

BlackCat is known for its ransomware being programmed in the Rust programming language and to encrypt different operating systems with great speed and stealth. The group is also known to operate a public leak site – in addition to one on the dark web – for added pressure on the victim.

After facing a law enforcement takedown in December 2023, the group announced an increase to the share received by affiliates and a reduction in targeting restrictions. It is believed that many affiliates have moved on to other ransomware-as-a-service operations and that the group may reemerge under a new brand.

Data availability

The authors do not have permission to share data.

References

Abdul G. & Milmo, D. (2024) Hacked London NHS hospitals data allegedly published online. Retrieved August 6, 2025, from The Guardian: https://www.theguardian.com/society/article/2024/jun/21/hacked-london-nhs-hospitals-data-allegedly-published-online.

Abrams, L. (2021a). Largest U.S. pipeline shuts down operations after ransomware attack. Retrieved August 27, 2024, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/.

Abrams, L., (2021b). Angry Conti Ransomware Affiliate Leaks Gang...s Attack Playbook. Retrieved August 27, 2024, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/.

Abrams, L. (2023). FBI disrupts Blackcat ransomware operation, creates decryption tool. Retrieved August 27, 2024, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/fbi-disrupts-blackcat-ransomware-operation-creates-decryption-tool/.

Abrams, L. (2025). M&S confirms social engineering led to massive ransomware attack. Retrieved July 9, 2025, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/mands-confirms-social-engineering-led-to-massive-ransomware-attack/.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D., 2018. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 4 (1).

Ahmad, R., Yunos, Z., Sahib, S., 2012. Understanding cyber terrorism: the grounded theory method applied. In: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE, pp. 323–328.

Akamai. (n.d.). What is BlackCat Ransomware? Retrieved September 7, 2024, from Akamai: https://www.akamai.com/glossary/what-is-blackcat-ransomware.

Arghire, I. (2024). RansomwareBlackCat ransomware successor Cicada3301 emerges. Retrieved November 7, 2024, from Security Week: https://www.securityweek.com/blackcat-ransomware-successor-cicada3301-emerges/.

Barry, C. (2024). ALPHV-BlackCat ransomware group goes dark. Retrieved August 25, 2024, from Barracuda: https://blog.barracuda.com/2024/03/06/alphv-blackcat-ransomware-goes-dark.

BBC. (2022). BA tries to poach rival cabin crew staff with £1000 bonus. Retrieved August 23, 2024, from BBC News: https://www.bbc.co.uk/news/business-61104230.

Benge, A. (2023). BlackCat (ALPHV): what we know about the MGM hack. Retrieved September 7, 2024, from ReversingLabs: https://www.reversinglabs.com/blog/what-we-know-about-blackcat-and-the-mgm-hack.

Bhasin, K. (2011). The 12 most intense marketing wars ever. Retrieved September 7, 2024, from Business Insider: https://www.businessinsider.com/epic-marketing-wars-2011-6.

Bing, C. (2022). Russia-based ransomware group Conti issues warning to Kremlin foes. Retrieved September 7, 2024, from Reuters: https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

Borges, E. (2024). Most popular ransomware groups. Retrieved from Recorded Future: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-groups.

Boticiu, S., Teichmann, F., 2023. How does one negotiate with ransomware attackers? Int. Cybersecur. Law Rev. 5, 55–65. https://doi.org/10.1365/s43439-023-00106-w.

Boustead, A.E., Herr, T., 2020. Analyzing the ethical implications of research using leaked data. PS: Polit. Sci. Polit. 53 (3), 505–509.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Braun, V., Clarke, V., 2012. Thematic analysis. In: Cooper, H., Camic, P.M., Long, D.L., Panter, A.T., Rindskopf, D., Sher, K.J. (Eds.), APA Handbook of Research Methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and Biological. American Psychological Association, pp. 57–71. https://doi.org/10.1037/13620-004, 71. https://psycnet.apa.org/record/2011-23864-004.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., 2014. An analysis of the nature of groups engaged in cyber crime. An analysis of the nature of groups engaged in cyber crime. Int. J. Cyber Criminol. 8 (1), 1–20.

Brown, R., Pehrson, S., 2019. Group processes: Dynamics within and Between Groups. John Wiley & Sons.

Bryman, A., 2016. Social Research Methods. Oxford university press.

Burgess, M. (2022a). The workaday life of the world's most dangerous ransomware gang. Retrieved September 7, 2024, from Wired: https://www.wired.com/story/conti-leaks-ransomware-work-life/.

Burgess, M. (2022b). Conti's attack against Costa Rica sparks a new ransomware era. Retrieved October 25, 2024, from Wired: https://www.wired.com/story/costa-rica-ransomware-conti/.

Burgess, M. (2024). A global police operation just took down the notorious LockBit ransomware gang. Retrieved August 25, 2024, from Wired: https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi/.

Canadian Centre for Cyber Security, 2023. Profile: ALPHV/BlackCat Ransomware. Canadian Centre for Cyber Security. Retrieved September 7, 2024, from. https://www.cyber.gc.ca/en/guidance/profile-alphvblackcat-ransomware.

Carlisle, D. (2023). Ransomware & crypto: the growing compliance challenge. Retrieved August 17, 2024, from Reuters: https://www.reuters.com/legal/legalindustry/ransomware-crypto-growing-compliance-challenge-2023-05-01/.

Center for Internet Security. (n.d.). Breaking down the BlackCat ransomware operation. Retrieved September 7, 2024, from Center for Internet Security: https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation.

Chainalysis. (2024a). Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 Decline. Retrieved September 9, 2024, from Chainalysis: https://www.chainalysis.com/blog/ransomware-2024/.

Chainalysis. (2024b). 2024 Crypto crime mid-year update part 1: cybercrime climbs as exchange thieves and ransomware attackers grow bolder. Retrieved September 9, 2024, from Chainalysis: https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/.

CheckPoint. (2022a). Check point research reveals leaks of Conti Ransomware group. Retrieved September 7, 2024, from Check Point: https://blog.checkpoint.com/security/check-point-research-revels-leaks-of-conti-ransomware-group/.

CheckPoint. (2022b). Leaks of Conti ransomware group paint picture of a surprisingly normal tech start-up… sort of. Retrieved August 25, 2024, from Check Point: https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/.

Cimpanu, C. (2021). Darkside ransomware gang says it lost control of its servers & money a day after Biden threat. Retrieved August 25, 2024, from The Record: https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat.

Cluley, G. (2024). The LockBit ransomware gang rears its ugly head again, after law enforcement takedown. Retrieved June 20, 2025, from Bitdefender: https://www.bitdefender.com/en-gb/blog/hotforsecurity/the-lockbit-ransomware-gang-rears-its-ugly-head-again-after-law-enforcement-takedown.

Cluley, G. (2025a). SafePay ransomware: what you need to know. Retrieved July 1, 2025, from Fortra: https://www.fortra.com/blog/safepay-ransomware-what-you-need-know.

Cluley, G. (2025b). AiLock ransomware: what you need to know. Retrieved July 5, 2025, from Fortra: https://www.fortra.com/blog/ailock-ransomware.

Coker, J. (2024). LockBit most prominent ransomware actor in May 2024. Retrieved August 25, 2024, from Infosecurity Magazine: https://www.infosecurity-magazine.com/news/lockbit-prominent-ransomware-may.

Coker, J. (2025). New hellcat ransomware gang employs humiliation tactics. Retrieved January 29, 2025, from Infosecurity Magazine: https://www.infosecurity-magazine.com/news/hellcat-ransomware-humiliation/.

Collier, K. (2024). Global law enforcement takes down ransomware group that targeted U.S. hospitals and schools. Retrieved August 25, 2024, from NBC News: https://www.nbcnews.com/tech/lockbit-ransomware-arrest-website-bust-rcna139533.

Connolly, L., Borrion, H., Arief, B., Kaddoura, S., 2023. Applying neutralisation theory to better understand ransomware offenders. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, pp. 177–182. https://doi.org/10.1109/EuroSPW59978.2023.00025. Delft.

Corera, G. (2024). Lockbit: UK leads disruption of major cyber-criminal gang. Retrieved September 7, 2024, from BBC News: https://www.bbc.co.uk/news/technology-68344987.

Counter Ransomware Initiative (CRI). (2023) Counter ransomware Initiative (CRI). Retrieved October 1, 2024, from CRI: https://counter-ransomware.org/aboutus.

Coveware. (2020). Ransomware demands continue to rise as Data Exfiltration becomes common, and Maze subdues. Retrieved October 7, 2024, from Coveware: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

Cyber Monitoring Centre (CMC). (2025). Cyber Monitoring Centre Statement on ransomware incidents in the retail sector – June 2025. Retrieved August 27, from CMC: https://cybermonitoringcentre.com/2025/06/20/cyber-monitoring-centre-statement-on-ransomware-incidents-in-the-retail-sector-june-2025/.

Cyberint. (2022). To Be CONTInued? Conti ransomware heavy leaks. Retrieved September 7, 2024, from Cyberint: https://cyberint.com/blog/research/contileaks/.

Cybersecurity & Infrastructure Security Agency (CISA). (2023a). #StopRansomware: LockBit 3.0. Retrieved September 7, 2024, from CyberSecurity & Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a.

Cybersecurity & Infrastructure Security Agency (CISA). (2023b). Understanding ransomware threat actors: lockBit. Retrieved September 7, 2024, from CyberSecurity & Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.

Cybersecurity & Infrastructure Security Agency (CISA). (2023c). #StopRansomware: Play Ransomware. Retrieved September 7, 2024, from CyberSecurity & Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a.

Cybersecurity and Infrastructure Security Agency (CISA). (2024a). #StopRansomware: ALPHV Blackcat. Retrieved August 25, 2024, from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a.

Cybersecurity and Infrastructure Security Agency (CISA). (2024b). #StopRansomware: ransomHub ransomware. Retrieved October 25, 2024, from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a.

Décary-Hétu, D., Dupont, B., 2013. Reputation in a dark network of online criminals. Glob. Crime 14 (2–3), 175–196.

Department of Justice (DOJ), US. (2021). Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists darkside. Retrieved August 21, 2024, from Office of Public Affairs, U.S. Department of Justice: https://www.justice.

gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
Department of Justice (DOJ), US. (2023). U.S. Department of Justice disrupts hive ransomware variant. Retrieved October 25, 2024, from Office of Public Affairs, U.S. Department of Justice: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.
Department of Justice (DOJ), US. (2024). Two foreign nationals plead guilty to participating in LockBit Ransomware Group. Retrieved October 25, 2024, from Office of Public Affairs, U.S. Department of Justice: https://www.justice.gov/opa/pr/two-foreign-nationals-plead-guilty-participating-lockbit-ransomware-group.
Deslandes, N., & Corvin, A.-M. (2022). Ransomware: the hackers and their marketplace. Retrieved August 25, 2024, from Tech Informed: https://techinformed.com/ransomware-the-hackers-and-their-marketplace/.
DiMaggio, J. (2023a). A behind the scenes look into investigating conti leaks. Retrieved August 25, 2024, from Medium: https://medium.com/ @jon.dimaggio/a-behind-the-scenes-look-into-investigating-conti-leaks-f57064a2afd2.
DiMaggio, J. (2023b). Ransomware Diaries: volume 1. Retrieved August 25, 2024, from Analyst1: https://analyst1.com/ransomware-diaries-volume-1/.
DiMaggio, J. (2023c). Ransomware Diaries: volume 2 – A Ransomware Hacker Origin Story. Retrieved August 25, 2024, from Analyst1: https://analyst1.com/ransomware-diaries-volume-2/.
Emisoft. (2019). Caution! Ryuk ransomware decryptor damages larger files, even if you pay. https://www.emsisoft.com/en/blog/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/.
eSentire. (2022). Conti ransomware gang claims 50+ new victims including oil terminal operator sea-invest disrupting operations at 24 seaports across Europe and Africa. Retrieved September 25, 2024, from eSentire: https://www.esentire.com/security-advisories/conti-ransomware-gang-claims-50-new-victims-including-oil-terminal-operator-sea-invest.
eSentire. (2023a). LockBit ransomware gang attacks an MSP and two manufacturers using RMM tools. Retrieved August 25, 2024, from eSentire: https://www.esentire.com/blog/russia-linked-lockbit-ransomware-gang-attacks-an-msp-and-two-manufacturers.
eSentire. (2023b). The notorious ALPHV/BlackCat ransomware gang is attacking corporations and public entities using Google ads laced with malware, warns eSentire. Retrieved September 7, 2024, from eSentire: https://www.esentire.com/blog/the-notorious-alphv-blackcat-ransomware-gang-is-attacking-corporations-and-public-entities-using-google-ads-laced-with-malware-warns-esentire.
European Union (EU). (n.d.). Glossary:commonwealth of Independent States (CIS). Retrieved August 9, 2024, from EU: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Commonwealth_of_Independent_States_(CIS).
Europol. (2024). Law enforcement disrupt world's biggest ransomware operation. Retrieved September 7, 2024, from Europol: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.
Europol. (2025). Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown. Retrieved July 1, 2025, from Europol: https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown.
Edwards, C. (2025). Co-op says cyber-attack cost it £206m in lost sales. Retrieved August 8, 2025, from BBC: https://www.bbc.co.uk/news/articles/ckgq9dke4e5o.
Farrell, J. (2024). Change Healthcare blames 'Blackcat' Group for cyber attack that disrupted pharmacies and health systems. Retrieved September 7, 2024, from Forbes: https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/.
Fereday, J., Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. Int. J. Qual. Methods 5 (1), 80–92. https://doi.org/10.1177/160940690600500107.
Ferguson-Walter, K.J., Major, M.M., Johnson, C.K., Johnson, C.J., Scott, D.D., Gutzwiller, R.S., Shade, T., 2023. Cyber expert feedback: experiences, expectations, and opinions about cyber deception. Comput. Secur. 130, 103268.
Ficara, A., Curreri, F., Fiumara, G., De Meo, P., 2023. Human and social capital strategies for Mafia network disruption. IEEE Trans. Inf. Forensics Secur. 18, 1926–1936.
Fier, J. (2021, December 7). Conti ransomware group finds new double extortion avenues. Retrieved September 7, 2024, from DarkTrace: https://darktrace.com/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation.
Flashpoint. (2021). Disgruntled Conti affiliate leaks ransomware training documents. Retrieved August 25, 2024, from Flashpoint: https://flashpoint.io/blog/disgruntled-conti-affiliate-leaks-ransomware-training-documents/.
Flashpoint. (2022). Conti ransomware: inside one of the world's most aggressive ransomware groups. Retrieved August 25, 2024, from FlashPoint: https://flashpoint.io/blog/history-of-conti-ransomware/.
Flashpoint. (2023). LockBit Ransomware: inside the world's most active ransomware group. Retrieved from Flashpoint: https://flashpoint.io/blog/lockbit/.
Geary, C. (2023). Lockbit ransomware gang - longevity or downfall? Retrieved September 7, 2024, from ThreatSpike: https://www.threatspike.com/blogs/lockbit-ransomware-gang.
Gray, I.W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2022). Money over morals: a business analysis of Conti ransomware. 2022 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1–12). Boston: IEEE. doi:10.1109/eCrime57793.2022.10142119.
Greig, J. (2024). Europol, DOJ, NCA deny involvement in recent AlphV/BlackCat 'shutdown'. Retrieved August 25, 2024, from The Record: https://therecord.media/europol-doj-nca-deny-involvement-in-alphv-blackcat-ransomware-takedown.
Greig, J. (2025a). IT company Ingram Micro says ransomware targeted internal systems. Retrieved June 2, 2024, from https://therecord.media/ingram-micro-ransomware-attack.
Greig, J. (2025b). Two Russian nationals arrested in takedown of Phobos ransomware infrastructure. Retrieved April 2, 2024, from The Record: https://therecord.media/phobos-ransomware-takedown-arrests-russian-nationals.
Grossman, T., & Smith, T. (2024). 2023 RTF global ransomware incident map: attacks increase by 73%, big game hunting appears to surge. Retrieved from Institute for Security and Technology: https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map/.
Gutierrez, A. (2025). CBS Evening News cyberattack that crippled Nevada's systems reveals vulnerability of smaller government agencies to hackers. Retrieved August 26, 2025, from CBS News: https://www.cbsnews.com/news/cyberattack-cripples-nevada-state-systems/.
Harpur, R. (2024). Ransomware focus: lockBit attacks in 2024. Retrieved September 9, 2024, from BlackFog: https://www.blackfog.com/lockbit-attacks-2024/.
Heimdal. (2024). All about Conti ransomware. From $180 million yearly revenue to internal data leakage. Retrieved September 7, 2024, from Heimdal: https://heimdalsecurity.com/blog/what-is-conti-ransomware/.
Hill, J. (2023). BlackCat Ransomware (ALPHV). Retrieved September 7, 2024, from Varonis: https://www.varonis.com/blog/blackcat-ransomware.
Hostetler, S. & Campbell, S. (2024). Follow-on extortion campaign targeting victims of Akira and royal ransomware. Retrieved July 17, 2024, from Arctic Wolf: https://arcticwolf.com/resources/blog/follow-on-extortion-campaign-targeting-victims-of-akira-and-royal-ransomware/.
Ikeda, S. (2022). Conti Ransomware group voluntarily shuttered, but members expected to splinter off to smaller groups. Retrieved September 7, 2024, from CPO Magazine: https://www.cpomagazine.com/cyber-security/conti-ransomware-group-voluntarily-shuttered-but-members-expected-to-splinter-off-to-smaller-groups/.
Ikeda, S. (2024). LockBit's claimed hack on US Federal Reserve turns out to Be a publicity stunt; stolen data came from just one US bank. Retrieved August 25, 2024, from CPO Magazine: https://www.cpomagazine.com/cyber-security/lockbits-claimed-hack-on-us-federal-reserve-turns-out-to-be-a-publicity-stunt-stolen-data-came-from-just-one-us-bank/.
Ilascu, I. (2024). BlackCat ransomware shuts down in exit scam, blames the "feds". Retrieved August 25, 2024, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds.
Imano, S. & Slaughter, J. (2022). Ransomware Roundup – Play. Retrieved September 20, 2024, from Fortinet: https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware.
Johansmeyer, T., Mott, G., Nurse, J.R., 2025. Invisible lines, visible impact: how territorial security influences Russian cyber security strategy. RUSI J 170 (1), 20–31.
Jones, C. (2023). BlackCat ransomware crims threaten to directly extort victim's customers. Retrieved September 7, 2024, from The Register: https://www.theregister.com/2023/12/05/alphvblackcat_shakes_up_tactics_again/.
Kaspersky. (2024a). State of ransomware in 2024. Retrieved August 25, 2024, from SecureList: https://securelist.com/state-of-ransomware-2023/112590/.
Kaspersky. (2024c). LockBit ransomware What You Need to Know. Retrieved September 7, 2024, from Kaspersky: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.
Kaspersky. (2024b). Understanding BlackCat ransomware: Threat overview and protective measures. Retrieved September 7, 2024, from Kaspersky: https://www.kaspersky.com/resource-center/threats/blackcat-ransomware.
Katagiri, N., 2023. From Prepaid Cards to bitcoin: How did Ransomware Hackers Adopt cryptocurrencies? Journal of Cyber Policy. https://doi.org/10.1080/23738871.2024.2435956.
Kerns, Q., Payne, B., Abegaz, T., 2021. Double-extortion ransomware: a technical analysis of maze ransomware. Proc. Future Technol. Conf. (FTC) 360, 82–94. https://doi.org/10.1007/978-3-030-89912-7_7. Springer.
Kim, G., Kim, S., Kang, S., Kim, J., 2022. A method for decrypting data infected with Hive ransomware. J. Inf. Secur. Appl 71. https://doi.org/10.1016/j.jisa.2022.103387.
Kovacs, E. (2022). Conti ransomware operation shut down after brand becomes toxic. Retrieved September 7, 2024, from SecurityWeek: https://www.securityweek.com/conti-ransomware-operation-shut-down-after-brand-becomes-toxic/.
Kovacs, E. (2023). Law enforcement reportedly behind takedown of BlackCat/Alphv ransomware website. Retrieved September 7, 2024, from SecurityWeek: https://www.securityweek.com/law-enforcement-reportedly-behind-takedown-of-blackcat-alphv-ransomware-website/.
Krebs, B. (2021). Ransomware gangs and the name game distraction. Retrieved August 25, 2024, from KrebsonSecurity: https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/.
Krebs, B. (2022). Conti Ransomware Group Diaries, part I to part IV. Retrieved September 7, 2024, from KrebsonSecurity: https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/, https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/, https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/, https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/.
Krebs, B. (2023). BlackCat ransomware raises ante after FBI disruption. Retrieved September 7, 2024, from KrebsonSecurity: https://krebsonsecurity.com/2023/12/blackcat-ransomware-raises-ante-after-fbi-disruption/.

Krebs, B. (2024). Category archives: ransomware. Retrieved August 25, 2024b, from KrebsonSecurity: https://krebsonsecurity.com/category/ransomware/.
Lakshmanan, R. (2023). Play ransomware goes commercial - now offered as a service to cybercriminals. Retrieved July 21, 2024, from Hacker News: https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html.
Levison, J. (2024). Lockbit ransomware gang's origins, tactics and past targets - and what next after policing breakthrough. Retrieved September 6, 2024, from Sky News: https://news.sky.com/story/lockbit-ransomware-gangs-origins-tactics-and-past-targets-and-what-next-after-policing-breakthrough-13075988.
Leukfeldt, E.R., Lavorgna, A., Kleemans, E.R., 2017. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. Euro. J. Cri. Pol. Res. 23 (3), 287–300.
Lyngaas, S. (2024). FBI and allies seize dark-web site of world's most prolific ransomware gang. Retrieved September 7, 2024, from CNN: https://edition.cnn.com/2024/02/19/politics/fbi-ransomware-lockbit-dark-web-site/index.html.
MalwareHunterTeam. (2023). BlackCat ransomware gang says that they just reported… retrieved August 22, 2024, from Twitter/X: https://x.com/malwrhunterteam/status/1724902112755384487.
Martin, J., Whelan, C., 2023. Ransomware through the lens of state crime: conceptualizing ransomware groups as cyber proxies, pirates, and privateers. J. Int. State Crime Initiat. 12 (1).
Martin, J., Whelan, C., Bright, D., 2024. Ransomware HR: human resources practices and organizational support in the Conti Ransomware group. Deviant Behav. 1–16. https://doi.org/10.1080/01639625.2024.2419905.
Martinez, F. (2022). BlackCat ransomware. Retrieved August 25, 2024, from LevelBlue: https://cybersecurity.att.com/blogs/labs-research/blackcat-ransomware.
Matthijsse, S.R., van 't Hoff-de Goede, Leukfeldt, E.R., 2023. Your files have been encrypted: A crime script analysis of ransomware attacks. Trends Organiz. Crime 1–27.
Mavroeidis, V., Hohimer, R., Casey, T., Jesang, A., 2021. Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. 13th International Conference On Cyber Conflict (CyCon). IEEE, Tallinn, Estonia, pp. 327–352. Retrieved August 27, 2024, from. https://ieeexplore.ieee.org/document/9468305.
McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Halgamuge, M., 2024. Ransomware Reloaded: re-examining its trend, research and mitigation in the era of data exfiltration. ACM Comput. Surv. https://doi.org/10.1145/3691340.
Medlock, B. (2023). Conti ransomware: prepare and protect your clients. Retrieved September 7, 2024, from ConnectWise: https://www.connectwise.com/blog/cybersecurity/what-is-conti-ransomware-how-to-prepare.
Meegan-Vickers, J. (2023). The rise and fall of the Conti ransomware group. Retrieved August 25, 2024, from Global Initiative Against Transnational Organized Crime: https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/.
Meegan-Vickers, J. (2024). The LockBit takedown. Retrieved September 7, 2024, from Global Initiative Against Transnational Organized Crime: https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/.
Meland, P.H., Bayoumy, Y.F.F., Sindre, G., 2020. The ransomware-as-a-service economy within the darknet. Comput. Secur. 92, 101762.
Menn, J., & Sands, L. (2024). 11-nation operation takes down world's 'most harmful' cybercriminal group. Retrieved September 7, 2024, from The Washington Post: https://www.washingtonpost.com/business/2024/02/20/lockbit-ransomware-cronos-nca-fbi/.
Mersinas, K., Liu, A., & Panteli, N. (2024). Analysing the cultural dimensions of cybercriminal groups - A case study on the Conti ransomware group. Human Factor in Cybercrime (HFC) Conference.
Meurs, T., Junger, M., Tews, E., Abhishta, A., 2022. Ransomware: How attacker's effort, Victim Characteristics and Context Influence Ransom requested, Payment and Financial loss. 2022 APWG Symposium on Electronic Crime Research (eCrime). IEEE, Boston, pp. 1–13. https://doi.org/10.1109/eCrime57793.2022.10142138.
Mott, G., Turner, S., Nurse, J.R.C., MacColl, J., Sullivan, J., Cartwright, A., Cartwright, E., 2023. Between a rock and a hard(ening) place: cyber insurance in the ransomware era. Comput. Secur. 128. https://doi.org/10.1016/j.cose.2023.103162.
Mott, G., Turner, S., Nurse, J.R.C., Pattnaik, N., MacColl, J., Huesch, P., Sullivan, J., 2024. There was a bit of PTSD every time I walked through the office door': ransomware harms and the factors that influence the victim organization's experience. J. Cybersecur. 10 (1). https://doi.org/10.1093/cybsec/tyae013.
Muncaster, P. (2023). BlackCat ransomware group reports victim to SEC. Retrieved September 7, 2024, from Infosecurity Magazine: https://www.infosecurity-magazine.com/news/ransomware-group-reports-victim-to/.
Muncaster, P. (2024). Cicada3301 Ransomware group emerges from the ashes of ALPHV. Retrieved September 2, 2024, from InfoSecurity Magazine: https://www.infosecurity-magazine.com/news/cicada3301-ransomware-group-alphv/.
National Crime Agency (NCA). (2017). Pathways into cyber crime. Retrieved June 28, 2025, from National Crime Agency: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.
National Crime Agency (NCA). (2024a). International investigation disrupts the world's most harmful cybercrime group. Retrieved August 25, 2024, from National Crime Agency: https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group.
National Crime Agency (NCA). (2024b). LockBit leader unmasked and sanctioned. Retrieved August 25, 2024, from National Crime Agency: https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned.
National Cyber Security Centre (NCSC). (2024). Ransomware-resistant backups. Retrieved August 25, 2024, from NCSC: https://www.ncsc.gov.uk/collection/ransomware-resistant-backups/principles-for-ransomware-resistant-cloud-backups.
Nield, D. (2024) Samsung roasts Apple's lack of foldable innovation in new ad – as a flexible iPhone is tipped for 2027. Retrieved November 25, 2024, from TechRadar: https://www.techradar.com/phones/iphone/samsung-roasts-apples-lack-of-foldable-innovation-in-new-ad-as-a-flexible-iphone-is-tipped-for-2027.
Nurse, J.R.C., Bada, M., 2018. The group element of cybercrime: types, dynamics, and criminal operations. The Oxford handbook of Cyberpsychology. Oxford University Press, pp. 691–715.
Ouellet, M., Hashimi, S., 2019. Criminal group dynamics and network methods. Methods of Criminology and Criminal Justice Research. Emerald Publishing Limited, pp. 47–65.
Oz, H., Aris, A., Levi, A., Uluagac, A.S., 2022. A survey on ransomware: evolution, taxonomy, and defense solutions. ACM Comput. Surv. (CSUR) 1–37.
Paarlberg, M.A., 2022. Transnational gangs and criminal remittances: a conceptual framework. Comp. Migr. Stud 10 (1), 24.
Paganini, P. (2024). Ukraine Police arrested a hacker who developed a crypter used by Conti and LockBit ransomware operation. Retrieved August 25, 2024, from SecurityAffairs: https://securityaffairs.com/164475/breaking-news/developer-crypter-conti-lockbit-ransomware.html.
Page, M.J. (2021). PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. doi: https://doi.org/10.1136/bmj.n160.
Paquet-Clouston, M., Haslhofer, B., Dupont, B., 2019. Ransomware payments in the Bitcoin ecosystem. J. Cybersecur. 5. https://doi.org/10.1093/cybsec/tyz003, 1. OUP.
Paternoster, C., Nazzari, M., Jofre, M., & Uberti, T.E. (2024). Inside the leak: exploring the structure of the Conti ransomware group. CrimRxiv. doi: https://doi.org/10.21428/cb6ab371.75a348ed.
Patterson, C.M., Nurse, J.R.C., Franqueira, V.N., 2023. Learning from cyber security incidents: a systematic review and future research agenda. Comput. Secur. 132. https://doi.org/10.1016/j.cose.2023.103309.
Patterson, C.M., Nurse, J.R.C., Franqueira, V.N., 2024. I don't think we're there yet": the practices and challenges of organisational learning from cyber security incidents. Comput. Secur. 139. https://doi.org/10.1016/j.cose.2023.103699.
Pattnaik, N., Nurse, J.R.C., Turner, S., Mott, G., MacColl, J., Huesch, P., Sullivan, J., 2023. It's more than just money: the real-world harms from ransomware attacks. Human aspects of information security and assurance. Springer 674, 261–274. https://doi.org/10.1007/978-3-031-38530-8_21.
Plumb, T. (2022). Lockbit 3.0 and the ransomware business model. Retrieved August 25, 2024, from VentureBeat: https://venturebeat.com/security/lockbit-3-0-and-the-ransomware-business-model/.
Poireault, K. (2024). LockBit admins tease a new ransomware version. Retrieved December 21, 2024, from Infosecurity: https://www.infosecurity-magazine.com/news/lockbit-admins-tease-a-new/.
PRISMA. (2020). PRISMA Statement. Retrieved August 25, 2024, from PRISMA Statement: https://www.prisma-statement.org/.
PSBE Cyber News Group. (2022). Conti ransomware attack causes State of emergency in Costa Rica! Retrieved September 7, 2024, from PSBE Cyber News Group: https://www.cybernewsgroup.co.uk/2022/05/11/conti-ransomware-attack-causes-state-of-emergency-in-costa-rica/.
Quorum Cyber. (n.d.). ALPHV threat actor profile. Retrieved September 7, 2024, from Quorum Cyber: https://www.quorumcyber.com/threat-actors/alphv-threat-actor-profile/.
Reddick, J. (2024). Teenage suspect in MGM Resorts hack arrested in Britain. Retrieved October 7, 2024, from The Record: https://therecord.media/mgm-hack-teenager-arrest-britain.
Ritchie, M.J., Drummond, K.L., Smith, B.N., Sullivan, J.L., Landes, S.J., 2022. Development of a qualitative data analysis codebook informed by the i-PARIHS framework. Implement. Sci. Commun. 3 (1), 98.
Ro, C. (2024). Why some cyber-attacks hit harder than others. Retrieved October 11, 2024, from The BBC: https://www.bbc.co.uk/news/business-68225892.
Rosendahl, T., & Burton, H. (2024). The LockBit story: why the ransomware affiliate model can turn takedowns into disruptions. Retrieved September 7, 2024, from Cisco Talos Blog: https://blog.talosintelligence.com/ransomware-affiliate-model/.
Ruellan, E., Paquet-Clouston, M., Garcia, S., 2024. Conti Inc.: understanding the internal discussions of a large ransomware-as-a-service operator with machine learning. Crime Sci 13 (16). https://doi.org/10.1186/s40163-024-00212-y.
Sangfor. (2022). Conti ransomware attack throws Costa Rica into a national State of emergency. Retrieved August 25, 2024, from Sangfor: https://www.sangfor.com/blog/cybersecurity/conti-ransomware-attack-throws-costa-rica-national-state-emergency.
Sangfor. (2024). LockBit group resurfaces after its recent takedown by US and UK law enforcers. Retrieved September 7, 2024, from Sangfor: https://www.sangfor.com/blog/cybersecurity/lockbit-ransomware-group-taken-down-us-and-uk-enforcers-announce.
SC Media. (2023). Hacker group files SEC complaint against its own victim. Retrieved September 7, 2024, from SC Media: https://www.scworld.com/news/hacker-group-files-sec-complaint-against-its-own-victim.
Scroxton, A. (2024). Royal ransomware crew puts on a BlackSuit in rebrand. Retrieved August 25, 2024, from Computer Weekly: https://www.computerweekly.com/news/366602360/Royal-ransomware-crew-puts-on-a-BlackSuit-in-rebrand.
Seals, T. (2024). LockBit ransomware takedown strikes deep into brand's viability. Retrieved August 25, 2024, from Dark Reading: https://www.darkreading.com/threat-intelligence/lockbit-ransomware-takedown-strikes-brand-viability.
Secureworks. (2023). Law enforcement takes action against ALPHV/BlackCat ransomware. Retrieved August 25, 2024, from Secureworks: https://www.secureworks.com/blog/law-enforcement-takes-action-against-alphv-blackcat-ransomware.
Securin. (2022). All about Conti ransomware. Retrieved August 25, 2024, from Securin: https://www.securin.io/articles/all-about-conti-ransomware/.

Securin. (2023). All about LockBit ransomware. Retrieved August 25, 2024, from Securin: https://www.securin.io/articles/all-about-lockbit-ransomware/.
Sergi, A., Storti, L., 2021. Shaping space. A conceptual framework on the connections between organised crime groups and territories: an introduction to the special issue on 'Spaces of Organised Crime. Trends Organ. Crime 24, 137–151.
Sharma. (2024). LockBit lied: stolen data is from a bank, not US Federal Reserve. Retrieved July 22, 2024, from BleepingComputer: https://www.bleepingcomputer.com/news/security/lockbit-lied-stolen-data-is-from-a-bank-not-us-federal-reserve/.
SOCRadar. (2022). Dark Web Profile: blackCat (ALPHV). Retrieved September 7, 2024, from SOCRadar: https://socradar.io/dark-web-profile-blackcat-alphv/.
SOCRadar. (2023). Dark web profile: lockBit 3.0 ransomware. Retrieved September 7, 2024, from SOCRadar: https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/.
Sophos. (2025). The State of Ransomware 2025. https://www.sophos.com/en-us/content/state-of-ransomware.
Symantec. (2022). Noberus ransomware: darkside and BlackMatter successor continues to evolve its tactics. Retrieved August 25, 2024, from https://symantec-enterprise-blogs.security.com/threat-intelligence/noberus-blackcat-ransomware-ttps.
Tanner, A., Hinchliffe, A., Santos, D., 2022. Threat assessment: blackCat ransomware. Retrieved August 25, 2024, from Unit 42. https://unit42.paloaltonetworks.com/blackcat-ransomware/.
Tata Communications. (2024). Unmasking the black cat ransomware: a deep dive into the threat. Retrieved September 7, 2024, from Tata Communications: https://www.tatacommunications.com/knowledge-base/guide-to-blackcat-ransomware-attacks/.
Temple-Raston, D., & Powers, S. (2024). Exclusive: after LockBit's takedown, its purported leader vows to hack on. Retrieved August 25, 2024, from The Record: https://therecord.media/after-lockbit-takedown-its-purported-leader-vows-to-hack-on.
Temple-Raston, D., Powers, S., & Abdul-Malik, J. (2024). In interview, LockbitSupp says authorities outed the wrong guy. Retrieved August 25, 2024, from The Record: https://therecord.media/lockbitsupp-interview-ransomware-cybercrime-lockbit.
The British Library. (2024). Learning lessons from the cyber-attack. Retrieved July 7, 2025, from The British Library: https://blogs.bl.uk/living-knowledge/2024/03/learning-lessons-from-the-cyber-attack.html.
The Guardian. (2021). Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack. Retrieved August 25, 2024, from The Guardian: https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom.
Thomas, D.R., Pastrana, S., Hutchings, A., Clayton, R., Beresford, A.R., 2017. Ethical issues in research using datasets of illicit origin. In: Proceedings of the 2017 Internet Measurement Conference, pp. 445–462.
Tidy, J. (2023). Ransomware hackers 'wreaking havoc' arrested in Ukraine. Retrieved October 22, 2024, from BBC: https://www.bbc.co.uk/news/technology-67556607.
Tologonov, J., & Fokker, J. (2024). The LockBit's attempt to stay relevant, its imposters and new opportunistic ransomware groups. Retrieved September 7, 2024, from Trellix: https://www.trellix.com/blogs/research/the-lockbits-attempt-to-stay-relevant-its-imposters-and-new-opportunistic-ransomware-groups/.
Toulas, B. (2024). Russian ransomware gangs account for 69% of all ransom proceeds. Retrieved October 7, 2024, from Bleeping Computer: https://www.bleepingcomputer.com/news/security/russian-ransomware-gangs-account-for-69-percent-of-all-ransom-proceeds/.
TrendMicro. (2022a). LockBit, Conti, and BlackCat lead pack amid rise in active RaaS and extortion groups. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022.
TrendMicro. (2022b). Research: ransomware spotlight: blackCat. Retrieved September 7, 2024, from TrendMicro: https://www.trendmicro.com/vinfo/gb/security/news/ransomware-spotlight/ransomware-spotlight-blackcat.
TrendMicro. (2024). LockBit attempts to stay afloat with a new version. Retrieved September 7, 2024, from TrendMicro: https://www.trendmicro.com/en_gb/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html.
TRM. (2022). TRM analysis corroborates suspected ties between Conti and Ryuk ransomware groups and wizard spider. Retrieved September 7, 2024, from TRM: https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider.
Tsipershtein, M. & Ananin, E. (2025). Ransomware gangs collapse as Qilin seizes control. Retrieved 2025, from Cybereason: https://www.cybereason.com/blog/threat-alert-qilin-seizes-control.
Turvey, B.E., 2011. Criminal profiling: An introduction to Behavioral Evidence Analysis. Academic press.
UK Government. (2023). No place to hide: serious and organised crime strategy 2023 to 2028. Retrieved 2024, from GOV.UK: https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2023-to-2028/no-place-to-hide-serious-and-organised-crime-strategy-2023-to-2028-accessible-version#chapter-2-executive-summary.
UK Government. (2025). Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting. Retrieved June 27, 2025 from GOV.UK: https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible.
Unit 42. (2024). Jumpy Pisces engages in play ransomware. Retrieved June 10, 2025 from Unit 42: https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/.
Vicens, A. (2022). Conti ransomware group announces support of Russia, threatens retaliatory attacks. Retrieved September 7, 2024, from CyberScoop: https://cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/.
Wadhwani, S. (2023). LockBit apologizes for ransomware attack on hospital, releases free decryptor. Retrieved September 7, 2024, from SpiceWorks: https://www.spiceworks.com/it-security/security-general/news/lockbit-ransomware-apologizes-sickkids-decryptor/.
Wang, C., Lu, Z., 2018. Cyber deception: Overview and the Road Ahead, 16. IEEE Security & Privacy, pp. 80–85.
Warminsky, J. (2022). Notorious cybercrime gang Conti 'shuts down,' but its influence and talent are still out there. Retrieved August 7, 2024, from The Record: https://therecord.media/conti-ransomware-gang-digital-infrastructure-shut-down.
Whelan, C., Bright, D., Martin, J., 2024. Reconceptualising organised (cyber)crime: the case of ransomware. J. Criminol. 57 (1), 45–61. https://doi.org/10.1177/26338076231199793.
Winder, D. (2024). Ransomware hackers fail to produce 'stolen' Donald Trump court files. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2024/02/29/stolen-donald-trump-court-files-will-be-published-february-29-hackers-say/.
Zimba, A., Chishimba, M., 2019. On the economic impact of crypto-ransomware attacks: the State of the art on enterprise systems. Eur. J. Secur. Res. 4, 3–31. https://doi.org/10.1007/s41125-019-00039-8.