



Kent Academic Repository

Lyne, Will, MacColl, Jamie and Nurse, Jason R. C. (2026) *From malware to marketplaces: The crossover between crime and state cyber activity*. RUSI Journal . ISSN 0307-1847.

Downloaded from

<https://kar.kent.ac.uk/115647/> The University of Kent's Academic Repository KAR

The version of record is available from

<https://doi.org/10.1080/03071847.2026.2683256>

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

CC BY (Attribution)

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in **Title of Journal** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).



From Malware to Marketplaces: The Crossover Between Crime and State Cyber Activity

Will Lyne, Jamie MacColl & Jason R C Nurse

To cite this article: Will Lyne, Jamie MacColl & Jason R C Nurse (16 Jun 2026): From Malware to Marketplaces: The Crossover Between Crime and State Cyber Activity, The RUSI Journal, DOI: [10.1080/03071847.2026.2683256](https://doi.org/10.1080/03071847.2026.2683256)

To link to this article: <https://doi.org/10.1080/03071847.2026.2683256>



Published online: 16 Jun 2026.



Submit your article to this journal [↗](#)



Article views: 14



View related articles [↗](#)



View Crossmark data [↗](#)



UK Prime Minister Keir Starmer visits Jaguar Land Rover, April 2025, prior to the cyberattack. Courtesy of PA Images/Alamy.

From Malware to Marketplaces

The Crossover Between Crime and State Cyber Activity

Will Lyne, Jamie MacColl and Jason R C Nurse

Technological change has transformed cybercrime from a niche issue to a national security problem. The shift has also narrowed the historic capability gap between criminal and state cyber actors to the point where threats such as ransomware pose some of the most acute cyber risks that nations face today. Although not identical, there are implications for how governments respond, given existing cyber strategies largely delineate between criminality and state threats.

The Landscape in the 2000s and Early 2010s

When the first UK Cyber Security Strategy was published in 2009, state cyber threat actors often ran sophisticated attacks known as advanced persistent threats (APTs) and represented the most significant cybersecurity risk. In 2010, the cybersecurity firm Mandiant published their first report on APT1, a Chinese state cyber group responsible for extensive cyber espionage campaigns against a range of victims from the UN to US defence contractors.¹

At the same time, banking malware was the priority cybercrime threat, which extensively targeted global victims for financial gain. The group operating the Zeus banking malware variant, for example, was disrupted by law enforcement in 2010 for the theft of US\$70 million, mostly from medium-sized companies and organisations such as churches.²

There was little apparent crossover. From 2010 onwards, online cybercrime marketplaces also grew in popularity. These allowed threat actors to exchange information, trade tools and capabilities for use in cybercrime operations. However, this cybercrime ecosystem was still immature, with high barriers to entry and lower sophistication tools and capabilities.

The dominant Russian-speaking cybercrime groups operated largely in vertically integrated organisational structures where the capabilities required to run operations were developed and then deployed by people in-house. They needed credibility, expertise and native Russian-language skills to access elite cybercrime platforms. It was also difficult for criminal actors who value anonymity to trade within the marketplace and realise profits from their crimes. Money muling

1. National Security Archive, 'Document 83', 1 February 2013, <<https://nsarchive.gwu.edu/document/21484-document-83>>, accessed 21 April 2026.
2. Federal Bureau of Investigation, 'Cyber Banking Fraud', <<https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud>>, accessed 21 April 2026.

(a way of cashing out ill-gotten funds) and reshipping schemes were slow, lacked capacity and were vulnerable to law enforcement disruption.

In addition, their technological methods were relatively unsophisticated. Although malware such as Zeus was available as a subscription service from around 2011, most capabilities were less pernicious. Denial of service tools such as the 'low orbit ion canon', which were used extensively in 2010 to target high profile websites, was temporarily disruptive but easy to mitigate and posed a low risk to most information and communication technology systems.³

Cybercrime Transformed

The adoption of new technologies transformed the cybercrime landscape in the mid-2010s. Cybercriminals embraced cryptocurrencies, which provided a common, reliable way to trade within the cybercrime ecosystem while maintaining anonymity, and enabled a quick, cheap, low risk way to cashout profits. This lifted the limitations on some cybercriminal operations leading to diversification into new types of criminal business models, including early ransomware. In 2013, CryptoLocker used strong encryption to lock victim devices and accepted ransoms in Bitcoin.⁴

Throughout the 2010s, the online cybercrime ecosystem expanded significantly and by 2020, ransomware was the most profitable and dominant cybercrime business model. Using dark web forums and communication channels, criminals could increasingly connect, share knowledge and trade in a way that enabled and supported their operations.

This both lowered the barrier of entry into cybercrime and proliferated increasingly sophisticated technical capabilities. Cybercrime escalated significantly as global internet access increased, and cybercriminals took particular advantage of the global pandemic.

Ransomware now poses a serious national security threat and is responsible for some of most high-profile cyberattacks in the UK.⁵

Why Cybercrime is a National Security Threat

There are two main reasons why cybercrime such as ransomware is now a national security threat. The first stems from the fact that cybercriminals possess significant capabilities and capacity enabling them to commit harm and at a much greater scale. The maturing of the ecosystem over the last decade has been such that criminals have a vast and accessible range of high-end criminal capabilities available through the commoditised and affordable 'as-a-service' model.⁶ This allows criminals to quickly access phishing kits, ransomware, botnets, hacking and exploits, and hosting infrastructure as and when they want it. The result has been attacks that cripple organisations, critical national infrastructure and governments, as can be seen in the attacks on Colonial Pipeline, Change Healthcare, Equifax, London Hospitals (Synnovis), and the Costa Rican government. These attacks can harm individual citizens but also can significantly impact a country's economy; the attack on Jaguar Land Rover, for example, is estimated to have cost the UK economy almost £2 billion.⁷

3. IT News, 'Anonymous Hackers Indicted for Operation Payback', <<https://www.itnews.com.au/news/anonymous-hackers-indicted-for-operation-payback-359381>>, accessed 21 April 2026.

4. Bitdefender, 'Cryptolocker Ransomware Makes a Bitcoin Wallet Per Victim', <<https://www.bitdefender.com/en-gb/blog/labs/cryptolocker-ransomware-makes-a-bitcoin-wallet-per-victim>>, accessed 21 April 2026.

5. UK Parliament, Joint Committee on the National Security Strategy, 'A Hostage to Fortune: Ransomware and UK National Security: Government Response to the Committee's First Report: Second Special Report of Session 2023–24', February 2024, <<https://publications.parliament.uk/pa/jt5804/jtselect/jtnatsec/601/report.html>>, accessed 21 April 2026; National Cyber Security Centre, 'NCSC Warns Enduring Significant Threat to UK's Critical Infrastructure', 14 November 2023, <<https://www.ncsc.gov.uk/pdfs/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure.pdf>>, accessed 21 April 2026.

6. Europol, '3.1 Crime-as-a-Service', Internet Organised Crime Threat Assessment, 2014, <<https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html>>, accessed 21 April 2026.

7. *The Guardian*, 'Jaguar Land Rover Hack Has Cost UK Economy £1.9bn, Most Costly Cyber-Attack in Britain 22 October 2025'.

While states may have worked independently in the past, collaborating with criminals allows them to leverage their capabilities.

The second reason is the increasing collaboration between cybercriminals and state cyber actors. While states may have worked independently in the past, collaborating with criminals allows them to leverage their capabilities. Whereas in 2010 crossovers were largely unknown, there is now a better understanding of how they can interact. The Evil Corp group, for instance, is known to have had Russian state connections for years, likely facilitated through familial links, and a GRU officer was exposed as having been a senior member of a longstanding elite Russian-speaking forum.⁸ The DanaBot malware, also run by Russia-based cybercriminals, had a parallel espionage version, and Chinese state actors have been linked to the use of ransomware in several operations.⁹ As recently as 2026, reports have also emerged of Lazarus Group using Medusa ransomware as part of its attacks.¹⁰

With these two points in mind, it is understandable that national governments have labelled ransomware so prominently. The Westminster government calls it ‘the most acute cyber threat facing the UK’.¹¹

Implications for the Response

Technology has driven changes in the cyber threat in ways that have closed the gap between state and criminal adversaries. In delivering a response, it is important to reflect broader views of how threats operate and to prioritise according to the risk and harm they pose, rather than to whoever potentially conducted them. This is especially important in an environment in which attribution is tricky to ascertain.

It has been argued that there is a bias within the cybersecurity community towards prioritising advanced persistent threats over ‘mere’ cybercrime, but that is no longer possible.¹² It is important that our responses effectively bring together the right skills and expertise to counter threats that we face based on the threat and risk they pose as opposed to who may be behind an attack, especially in the ‘grey zone’ between criminal and state cyber operations. ■

Will Lyne is the head of Economic and Cybercrime in London’s Metropolitan Police and PhD candidate at the University of Cambridge.

Jamie McColl is a Senior Research Fellow in RUSI’s Cyber and Tech research group, where his interests include the role of emerging technologies in security and defence.

Jason R C Nurse is a Reader in Cybersecurity at the University of Kent and an Associate Fellow at RUSI.

-
8. National Crime Agency, ‘Evil Corp: Behind the Screens’, October 2024, <<https://www.nationalcrimeagency.gov.uk/who-we-are/publications/732-evil-corp-behind-the-screens/file>>, accessed 21 April 2026; Brian Krebs, ‘From Cybercrime Saul Goodman to the Russian GRU’, Krebs on Security, 7 February 2024, <<https://krebsonsecurity.com/2024/02/from-cybercrime-saul-goodman-to-the-russian-gru/>>, accessed 21 April 2026.
 9. US Attorney’s Office, Central District of California, ‘16 Defendants Federally Charged in Connection With DanaBot Malware Scheme That Infected Computers’, <<https://www.justice.gov/usao-cdca/pr/16-defendants-federally-charged-connection-danabot-malware-scheme-infected-computers>>, accessed 21 April 2026; *CyberScoop*, ‘Chinese Hackers are Increasingly Deploying Ransomware, Researchers Say’, <<https://cyberscoop.com/chinese-hackers-are-increasingly-deploying-ransomware-researchers-say/>>, accessed 21 April 2026.
 10. *The Record*, ‘North Korean Hackers Using Medusa Ransomware’, 24 February 2026, <<https://therecord.media/north-korean-hackers-using-medusa-ransomware>>, accessed 21 April 2026.
 11. UK Government, ‘UK Cracks Down on Ransomware Actors’, 9 February 2023, <<https://www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors>>, accessed 21 April 2026.
 12. Selena Larson, ‘Why Biasing Advanced Persistent Threats Over Cybercrime Security Risk’, *RUSI Commentary*, 16 December 2024, <<https://www.rusi.org/explore-our-research/publications/commentary/why-biasing-advanced-persistent-threats-over-cybercrime-security-risk>>, accessed 21 April 2026.