On the Effectiveness of Ransomware Decryption Tools

Burak Filiz[a], Budi Arief[b,*], Orcun Cetin[a], Julio Hernandez-Castro[b]

[a] *Sabancı University, Turkey*
[b] *University of Kent, United Kingdom*

Abstract

Ransomware is a type of malware that locks out its victim's access to their device or data – typically by encrypting files – and demands payment in exchange of restoring access. To fight the increasing threat posed by ransomware, security researchers and practitioners have developed decryption tools. These tools aim to help victims in recovering their data, generally by decrypting the compromised files without paying the ransom. Unfortunately, there has been minimal research on the effectiveness of decryption and recovery tools. There is a scant understanding regarding the extent to which these tools can actually recover compromised data.

The research presented in this work aims to cover this gap by providing an empirical study on these tools' effectiveness – in terms of decrypting and restoring compromised data. For doing so, we tested a total of 78 tools created by 11 security companies against 61 ransomware samples. That allows us to present an in-depth critical discussion of the real effectiveness of the recovery tools studied. We found that nearly half of the tools fail to recover compromised data satisfactorily. We conclude that there is still a lot of work to be done before these tools can make a real positive impact on ransomware victims. We finish our work by offering some additional insights and recommendations that could help in improving the effectiveness of ransomware decryption tools.

Keywords: ransomware, decryptor, tools, effectiveness, data recovery.

[*] Corresponding author
Email address: `b.arief@kent.ac.uk` (Budi Arief)

1. Introduction

Ransomware is a type of malware (malicious software) that restricts access to its victim's computing resources. It typically displays a message – a ransom note – that demands payment to restore data or the functionality of a compromised device [1]. In effect, this type of malware holds the victim's data to ransom. Simply put, ransomware is an extortion racket [2].

Ransomware can spread in a variety of ways, the two most common being by downloading malicious files via email attachments and by browsing infected websites [3]. It is frequently disguised as genuine software, and criminals often use various social engineering techniques to disseminate it. For example, they may pretend to be an organisation willing to help with computer issues or may masquerade as a law enforcement officer acting to protect you from criminals.

The first ransomware attack can be traced back to thirty years ago, when the target was the World Health Organization's international AIDS conference [4]. However, we can trace the rise of modern ransomware back to 2005 [5, 6]. Before then, ransomware attacks and their payment methods were not sophisticated enough. There were no readily-available untraceable or pseudo-anonymous methods for payment. Victims were instructed to pay by mailing pre-paid cards or via SMS text messaging. Attackers also used other ways, for example, requesting victims to call premium rate telephone numbers that would earn money (directly or indirectly) for the attacker. These schemes were suboptimal as they could link back to the attacker [7].

Payment methods became more anonymous in 2009, the year when Bitcoin – the first cryptocurrency – was launched. Bitcoin is slightly harder to trace, compared to previous methods used by attackers. There was a gradual increase in ransomware until 2013, the year when Cryptolocker, one of the most famous ransomware strains, was released in the wild. CryptoLocker completely revolutionised ransomware attacks [8]. For example, it used an asymmetric encryption method and introduced a new and better Graphical User Interface (GUI) to deliver a ransom note.

The threat of ransomware has been snowballing over the past few years. It has now become one of the top five cyber threats for business [9]. The global cost of ransomware attacks is predicted to reach $20 billion in 2021 [10], and this impact is expected to get worse every year. The health and financial sectors are among the top targets, and both have faced significant hits in the recent past. Ransomware attacks have also grown considerably in sophistication. Attackers frequently study their targets with care and then plan a comprehensive and targeted attack to cripple their whole digital infrastructure.

Ransomware can be divided into two main categories. The first is commonly known as *lockers*, while the second is called *crypto-ransomware* [3, 5]. Lockers prevent legitimate users from accessing the functionality of their system. Victims are unable to access their system because a password, a PIN or some other code created by the criminals stops them. On the other hand, crypto-ransomware encrypts files on the victims' system so that victims cannot access their data as they do not have the decryption key. In both cases, victims are asked to pay a ransom – typically via a cryptocurrency – to regain access to their system or files. The work presented in this paper focuses on the latter category of crypto-ransomware. This makes sense because there are typically other ways to bypass lockers without paying the ransom, unlike in the case of crypto-ransomware. New tools and techniques are continuously being developed and deployed for detecting and recovering from ransomware attacks. A particularly visible and worthy initiative is the "No More Ransom" (NMR) project [11, 12], which provides several free recovery tools for various ransomware strains. Many of the main law enforcement agencies and Security companies in Europe actively collaborate in this project.

Motivation. A myriad of anti-ransomware techniques has been developed for early detection and recovery of ransomware attacks. But, despite the increasing number of decryption tools available, there are still millions of victims who fall prey to these attacks every year. Unfortunately, a significant number of them are compelled to end up paying the ransom to cybercriminals. This fact puts the availability, effectiveness and usefulness of these detection and recovery tools into question.

To examine this problem further, we carried out an investigation with the overall aim of finding out some of the most relevant features of currently available decryption tools. In particular, we wanted *to understand the extent to which these are successful in providing access back to the data.* This work examined in detail whether currently available decryption tools were able to completely or partially recover data. This analysis would give us a good understanding of their effectiveness. To achieve this, we extensively tested the available decryption tools against the specific ransomware strains that each is supposed to counter.

Contributions. The main contributions of our paper are:

- A set of empirical data regarding the effectiveness of 78 ransomware decryption tools. These came from 11 security vendors and were tested against 61 ransomware samples.
- Insights into the limitations of currently available decryptors, along with suggestions on how these may be addressed to improve their effectiveness.

The rest of this paper is organised as follows. Section 2 focuses on the literature review and related work. It covers detection, prevention and post-detection techniques and strategies against ransomware. Section 3 outlines our methodology, mainly how we analysed the effectiveness of the currently available decryption tools. Section 4 presents the main results gathered through testing the effectiveness of the tools. Section 5 discusses our main findings, along with some insights and lessons learned. Section 6 provides an analysis of the limitations of the current work and some ideas for future research. Lastly, Section 7 concludes our paper and summarises our contributions.

2. Related Work

There have been quite a large number of research papers over recent years in the area of ransomware. They mainly cover techniques for detecting and preventing ransomware-based attacks. However, there have been far fewer reports on how to proceed and what might happen after the infection. In particular, there are almost none on how recovery may be conducted.

2.1. Detection and Prevention

Most of the research regarding ransomware focuses on technical methods to detect and prevent it [13].

Kharraz et al. [14] was the first to analyse an extensive collection of ransomware samples. They introduce a dynamic analysis system called "Unveil" that can detect both known and unknown ransomware families. The authors collected ransomware samples from public repositories and other forums, and these were then tested on Unveil. A total of 148,223 samples were tested, out of which 13,637 were ransomware, including 9,872 new ones, leading to an impressive 0% false-positive rate. Each instance was allowed to interact for no more than twenty minutes with the artificial environment. This environment was generated to provide a realistic look, so that ransomware will not be able to detect or evade it easily. The authors compared their detection results with Virus Total. They decided that if a sample detected by Unveil as ransomware was not classified as such by Virus Total, then it would be reported as a new detection.

After Unveil, Scaife et al. [15] further worked in the area of ransomware detection. They present "CryptoDrop", an early-warning detection system that will alert users if there is suspicious file activity in the system. CryptoDrop can halt a process that seems to be tampering with large amounts of user data. The decision of stopping the process is based on a set of behaviour indicators. Alerts will only be triggered for a broad set of files and not for a couple of files with suspicious activity. The authors explain that the system can be trained for rapid ransomware detection with low false positives by combining a group of indicators common to ransomware. Experimental analysis of CryptoDrop showed that it could stop ransomware from executing with a median loss of only ten files (out of nearly 5,100 available files). Final results confirmed that carefully analysing malicious behaviour can lead to an effective early detection system preventing loss of victims' data.

Continella et al. [16] proposed "ShieldFS" to enable recovery from a ransomware attack without the need to pay a ransom by copying a file when it is modified, storing the copy in a protected area and allowing any changes to be made to the original file. It uses an add-on driver to the Windows operating system, and it can detect new and previously known ransomware with an accuracy of 96.7%. To create a robust detection technique, the authors focused on both benign and malicious behaviour, by carrying out a large-scale data collection of I/O Request Packets (IRPs) generated by benign applications in real-world conditions. Around 1.7 billion IRPs produced by 2,245 different applications were included in their dataset.

Andronio et al. [17] proposed "HELDROID" for the detection of ransomware in Android OS. Similar to other research, HELDROID is also focused on analysing the malicious encrypting behaviour of ransomware. The authors employed three independent detectors, which can be executed in parallel. These include a threatening text detector (a text classification to detect coercion attempts), an encryption detector (that indicates encryption is being actively performed on files), and a locking detector (that checks if the application can lock the device and restrict the user from logging in). The authors suggest that HELDROID could be integrated into mobile anti-virus software. Alternatively, HELDROID can be deployed in multiple checkpoints offered by current app-distribution ecosystems. For example, HELDROID could be part of the app-vetting processes that performed by online marketplaces such as Google Play Store, or upon installation of the apps.

Most of the work in this area is focused on technical aspects, but some have also studied the human aspects of ransomware attacks. Sittig et al. [18] highlight that mitigation and prevention of ransomware requires a socio-technical approach with the active involvement of humans that have been effectively trained with adequate security practices.

Social engineering is considered a significant attack vector for spreading malware [19]. Hull et al. [3] highlight how, for example, universities can easily become targets for these attacks. This fact is in part due to details of staff being openly available, so they may become easy prey to social engineering campaigns. Therefore it is particularly necessary to deploy adequate security practices for users and members of large public organisations.

Luo and Liao [20] also emphasised that awareness and education is key to the prevention of ransomware attacks. If security practices are not good enough, then an employee's mistake could compromise the whole organisation.

Leah et al. [21] covered in detail the effects of a ransomware attack at a large academic institution in the US. Participants mentioned, during the survey and interview, how they only had implemented weak security practices before the ransomware attack. Those changed significantly after the attack. This change was mainly due to the perception about the likelihood of their devices being compromised going up considerably during the attack, only to decrease after it finished, but not to levels as low as before it.

Recently, Tang et al. [22] proposed an introspection-based approach to detect and analyse ransomware called RansomSpector. This approach detection mechanism is located in the hypervisor layer, and it analyses both the file and network activities of ransomware. Their evaluation with 2,117 recent ransomware sample demonstrated that introspection-based approach is quite promising in terms of detecting newly crafted ransomware.

2.2. Post-Infection

There has also been some research into post-infection activities. This area is more closely related to this work because it is concerned with decrypting and restoring the compromised data. Typically, the primary motivation of attackers is to obtain financial gain. Therefore, as long as they are getting paid, they will keep pursuing this profitable line of business and investing time and resources in more sophisticated malware.

One preventative measure that potential victims can use is to keep backups of their data. Once ransomware has infected their system, victims would have to rely on their backups to recover it. Kaspersky reported that 47% of Small and Medium Businesses spend several days to restore their encrypted data, and 25% spend several weeks [23]. If they have no backup (or if the ransomware has encrypted it) then victims are frequently left with no choice but to pay the ransom. This decision is arguable [24]. Several research papers, such as [25], have looked into the game-theoretic aspects behind paying or not the ransom demand. The general consensus is, however, ransoms should not be paid.

The No More Ransom project [11, 12] was established in July 2016 to help ransomware victims in recovering their files without paying any ransom. It was launched by Europol's European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands' police and McAfee. Victims can access the No More Ransom website [11] to find (if available) the decryption tool corresponding to the ransomware strain that has infected their machine. This allows victims to recover their data and, when successful, discourage them from paying the ransom. To remove the ransomware from their systems, victims are generally required to use a separate anti-malware tool after recovering their data. We describe in detail in the following sections how the decryption of ransomware via the decryption tools works.

3. Methodology

We evaluated the effectiveness of the ransomware decryption tools to find out the extent to which they are capable of recovering the victim's data. To achieve this, we set up an experimental environment with Windows 10 as the main/host Operating System (OS). We installed Microsoft's Hyper-V to create different virtual machines (VMs) with Windows OS (Windows 7 x86, Windows 10 x64). After creating the VMs, we populated them with dummy data using files with various extensions such as .docx, .xlsx, .pdf, .zip, .mp4, .csv, .txt, .png, .mp3 and .ppt. Moreover, we disabled the anti-malware services running on Windows 10, so that ransomware can easily interact with the environment.

The purpose of populating the VMs with dummy data and making them look like any regular PC was to minimise the risk of ransomware samples detecting the VM environment, which might make them hold back on the encryption process. It could also help in finding out which type of files were preferentially encrypted by the tested ransomware, and which were successfully decrypted by the tools. After successfully setting up the initial Windows 10 VM, a *differencing disk* feature in Hyper-V was used to create additional copies of the initial VMs for testing various ransomware binaries. This way we could gather information about changes made by each ransomware and then reverted the VM back to the original state; in other words, all the ransomware samples were tested in same conditions. We followed the same process while testing ransomware samples in Windows 7 environment.

Many ransomware strains use a Command and Control (C&C) server and report back to the criminal about the victim's machine. To ensure the C&C server is working and the ransomware can complete its encryption process, we connected the VMs to the internet through a dedicated DHCP server.

This procedure also alleviated the risk of spreading the ransomware, infecting other internal devices and reduced the effort to configure network settings for each machine. We then created a list of ransomware (n = 141) for which decryption tools had been made available and listed on the No More Ransom website.

In each case, we searched for various executable samples of the ransomware under study. We found 72 samples, out of which 61 worked and were able to encrypt the honeypot files in our experiment platform. Each sample was allowed to interact with the OS for 10 minutes to start encrypting the files; if it did not encrypt anything for 10 minutes, we deemed it to be not working. These samples were collected from malware analysis and submission portals such as Hybrid Analysis[1] and ANY.RUN[2]. We cross-checked the hash of each ransomware binary with Virus Total[3] to ensure that we had the right sample.

[1] https://www.hybrid-analysis.com

[2] https://any.run

[3] https://www.virustotal.com

Table 1: Results of the tools tested against the 61 ransomware samples

	Security Vendors										
Ransomware	Avast	Bitdefender	Bleeping Computer	CERT	Checkpoint/Cisco	Emsisoft	F-Secure	Kaspersky	Trend Micro	McAfee	Tesorion
AES_NI	●							○			
Alcatraz	●										
Alpha			●								
Amnesia						●					
Annabelle		●	●								
Aurora			●			●					
Avest						●					
Bart**	○										
BigBobRoss	●					●					
BTCWare	○										
CERBER V1									○		
CheckMail7						●					
Chernolocker						●					
Chimera								○	○		
Crypt888	○										
CryptoMix	○			○							
CrySIS								○	○		
Derialock			●								
Dharma								○			
DragonCyber						●					
EncrypTile	○										
Everbe 1.0			◓								

FenixLocker						●					
FilesLocker v1 & v2			○								
GandCrab		●									
GetCrypt						●					
Globe v3						●					
GlobeImposter						○					
Gomasom						●					
Hakbit						●					
HiddenTear	○		○								
HildaCrypt						○					
InsaneCrypt			●								
Iwanttits						●					
Jaff								●			
JavaLocker						●					
Jigsaw			○		●	●			●		
JSWorm v4.0						●					
LambdaLocker	○										
Loocipher						●					
Mapo				●							
Marlboro						◓					
Mira							●				
MirCop									●		
Mole				○							
Nemty											○
Noobcrypt	●										
Ouroboros		○									
Paradise						○					
Pewcrypt						●					
Puma*						○					

Rotor								○			
SpartCrypt						●					
Stampado						○			○		
Syrk						●					
TeslaCryptV1*					○				○		
TeslaCryptV4*					●			●	●	●	
Thanatos					◓						
XData								○			
XORIST						●			○		
Yatron								●			

Notes: ● = full decryption; ◓ = partial decryption; ○ = no decryption.

* = Ransomware strain worked exclusively on Windows 7.

** = Bitdefender ransomware decryptor for Bart was not included in this study, because while it worked partially in Windows 10 environment, it did not work at all during our testing in Windows 7 environment.

4. Results

We evaluated the effectiveness of 78 decryption tools produced by 11 security companies, against 61 ransomware samples. Table 1 shows the results of using the decryption tools against the 61 ransomware samples they target, where ● means full decryption, ◓ represents partial decryption, and ○ is for no decryption. Out of the 61 samples that worked and were able to encrypt the honey files in the study platform, 58 samples worked on Windows 10, and 3 exclusively on Windows 7. For some ransomware variants, we managed to find multiple decryptors listed in the No More Ransom website. Once we infected our testing environment with ransomware, we uploaded the encrypted file and the ransom note to the No More Ransom website. This was aimed at checking whether it can detect the correct ransomware strain.

Then, we downloaded the corresponding tool targeting that concrete strain from No More Ransom. For each tool, we carefully read the instructions by the authors to ensure that we understood the workings of the tool. Where necessary, we looked for further details on public forums.

Table 2: The tools categorised by their effectiveness

Ransomware	# Unique Tools	# Tools Used	Decryption		
			Full	Partial	No
Avast	11	11	4	0	7
Bitdefender	3	3	2	0	1
Bleeping Computer	6	9	5	1	3
Cert	3	3	1	0	2
Checkpoint/Cisco	3	4	2	1	1
Emsisoft	26	27	21	1	5
F-Secure	1	1	1	0	0
Kaspersky	1	9	3	0	6
Trend Micro	1	9	3	0	6
McAfee	1	1	1	0	0
Tesorion	1	1	0	0	1
Total	*57*	*78 (100%)*	*43 (55%)*	*3 (4%)*	*32 (41%)*

Table 2 shows the tools divided into three categories according to their effectiveness (Full Decryption, Partial Decryption, or No Decryption). Out of the 78 tools tested, only 55% (n = 43) were able to completely recover files, 4% (n = 3) tools recovered them partially and a shocking 41% (n = 32) did not recover any data. Out of the 61 samples, only 57% (n = 35) were successfully decrypted, and its data fully restored. We provide a brief description of the decryption categories below.

4.1. Full Decryption

As shown in Table 2, 55% (n = 43) of the tools belonged to this category. These were able to completely recover all files from the compromised system. This category consists of 4 tools created by Avast, two by Bitdefender, five by Bleeping Computer, two by Checkpoint/Cisco, 21 created by Emsisoft, three by Kaspersky, three by Trend Micro, and one each by F-Secure, McAfee and Cert.

4.2. Partial Decryption

We found that 4% (n = 3) of the tools belonged to this category. It includes tools that either failed to restore all encrypted files or those that claim to support the decryption of multiple ransomware strains but did not manage to decrypt all of them. This category consists of one tool each by Bleeping Computer, Checkpoint/Cisco and Emsisoft.

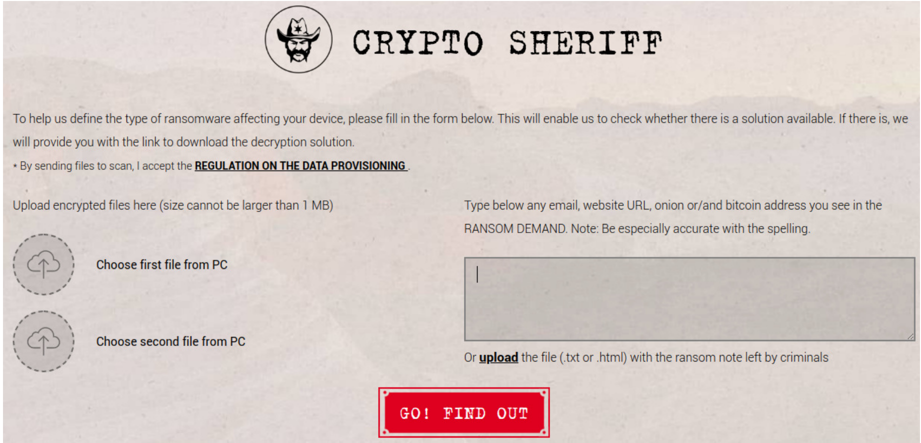
4.3. No Decryption

In terms of utter inability to decrypt, 41% (n = 32) of the tools belonged to this category. These tools did not manage to recover any encrypted file. They included seven by Avast, one by Bitdefender, three by Bleeping Computer, two by Cert, one by Checkpoint/Cisco, five by Emsisoft, six by Kaspersky, six by Trend Micro, and one by Tesorion.

4.4. Ransomware Identification Rates

The No More Ransom website offers a feature called "Crypto Sheriff", designed to identify a ransomware variant and suggest its corresponding decryption tool (see Figure 1). Crypto Sheriff attempts to identify the malware from the ransom note or some samples of encrypted files that a victim can upload to the site. We assessed the effectiveness of this feature by uploading both ransom notes and encrypted files by ransomware samples in our study.

We labelled as "correct identification" when Crypto Sheriff offered the correct decryptor associated with the ransomware note and encrypted files. Accordingly,



To help us define the type of ransomware affecting your device, please fill in the form below. This will enable us to check whether there is a solution available. If there is, we will provide you with the link to download the decryption solution.

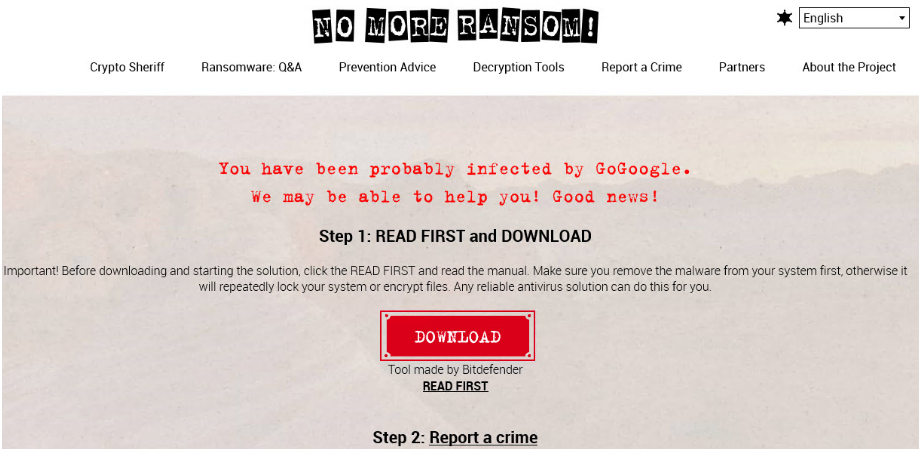
• By sending files to scan, I accept the **REGULATION ON THE DATA PROVISIONING**

Upload encrypted files here (size cannot be larger than 1 MB)

Type below any email, website URL, onion or/and bitcoin address you see in the RANSOM DEMAND. Note: Be especially accurate with the spelling.

Or **upload** the file (.txt or .html) with the ransom note left by criminals

Figure 1: Crypto Sheriff is used to identify the ransomware affecting victims' device



You have been probably infected by GoGoogle.
We may be able to help you! Good news!

Step 1: READ FIRST and DOWNLOAD

Important! Before downloading and starting the solution, click the READ FIRST and read the manual. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.

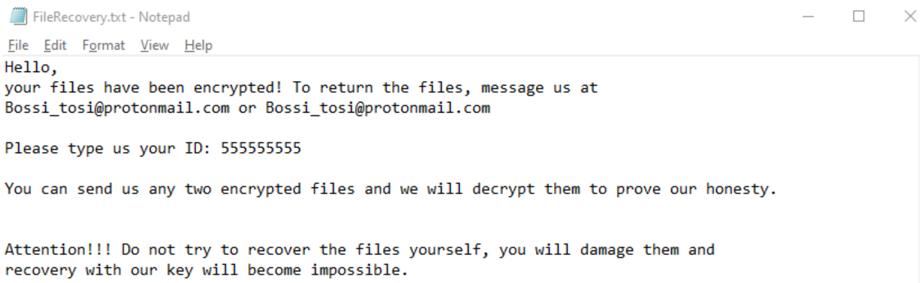
Tool made by Bitdefender
READ FIRST

Step 2: Report a crime

Figure 2: An example of incorrect identification by Crypto Sheriff, suggesting "GoGoogle" ransomwere while the ransom note actually came from "BigBobRoss" ransomware

"incorrect identification" referred to when Crypto Sheriff misidentified the sample or could not return any results claiming not to find an available decryptor. Lastly, "partially correct identification" was for when the Crypto Sheriff offered multiple solutions, and at least one of them linked to the correct decryptor.

Figure 2 shows an example of an incorrect ransomware identification. In this case, Crypto Sheriff misclassified the ransom note as belonging to the GoGoogle ransomware (the ransom note of which can be seen in Figure 3(a)) – and sug-



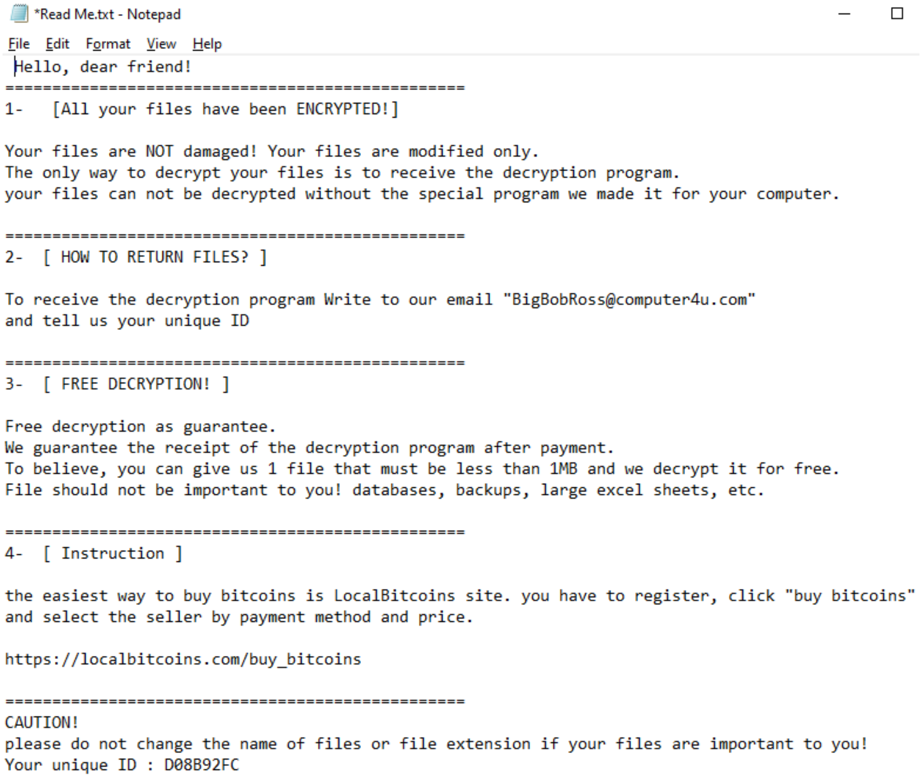
```
Hello,
your files have been encrypted! To return the files, message us at
Bossi_tosi@protonmail.com or Bossi_tosi@protonmail.com

Please type us your ID: 555555555

You can send us any two encrypted files and we will decrypt them to prove our honesty.


Attention!!! Do not try to recover the files yourself, you will damage them and
recovery with our key will become impossible.
```

(a) GoGoogle ransom note (taken from [26])



```
 Hello, dear friend!
==================================================
1-   [All your files have been ENCRYPTED!]

Your files are NOT damaged! Your files are modified only.
The only way to decrypt your files is to receive the decryption program.
your files can not be decrypted without the special program we made it for your computer.

==================================================
2-  [ HOW TO RETURN FILES? ]

To receive the decryption program Write to our email "BigBobRoss@computer4u.com"
and tell us your unique ID

==================================================
3-  [ FREE DECRYPTION! ]

Free decryption as guarantee.
We guarantee the receipt of the decryption program after payment.
To believe, you can give us 1 file that must be less than 1MB and we decrypt it for free.
File should not be important to you! databases, backups, large excel sheets, etc.

==================================================
4-  [ Instruction ]

the easiest way to buy bitcoins is LocalBitcoins site. you have to register, click "buy bitcoins"
and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

==================================================
CAUTION!
please do not change the name of files or file extension if your files are important to you!
Your unique ID : D08B92FC
```

(b) BigBobRoss ransom note (captured by our dynamic analysis)

Figure 3: Comparison of ransom notes for GoGoogle and BigBobRoss ransomware samples

gested the available solution for the GoGoogle ransomware – while in fact the ransom note was from BigBobRoss (seen in Figure 3(b)). Unfortunately but expectedly, the decryptor for GoGoogle can not recover the files encrypted by BigBobRoss. Meanwhile, the available solutions for BigBobRoss worked successfully and managed to decrypt all the compromised files.

Figure 4 shows the identification rates for the 61 variants used in our study. Out of the 61 uploaded encrypted files and ransom notes, only 43% (n = 26) were correctly identified by Crypto Sheriff, 49% (n = 30) were incorrectly identified and 8% (n = 5) were partially identified. In the majority of the cases, Crypto Sheriff did not manage to identify the correct version of the ransomware sample. This would likely cause victims to give up their search for available solutions while in fact, a solution may be easily accessible on the same website. As a result of this, victims might wrongly feel compelled to pay the ransom.

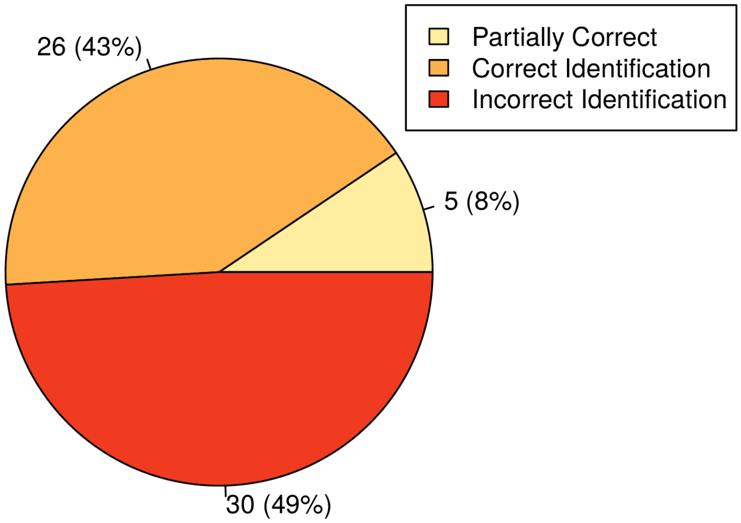


Figure 4: A breakdown of Crypto Sheriff's identification rates

4.5. Additional Resources Requested

In this section, we investigate the additional resources needed by the decryptors to recover the encrypted files. These requirements are another issue that could contribute to reducing decryptors' effectiveness, as users might not be, in many cases, able to provide the additional info requested.

Table 3 shows a summary of the additional resources requested by the decryptors in our study. We have obtained this information from the "How-to Guide" offered by the vendors. The results showed that 39 of the 78 decryptors

Table 3: The tools categorised by additional resources required to recover the files

Category	# **Decryptor**
No added requirements	39 (50%)
Encrypted and original files	23 (29.5%)
Only ransomware generated files	16 (20.5%)
– Ransom note	7 (9%)
– Ransomware key file	3 (3.8%)
– Original machine	3 (3.8%)
– Recover the Master Boot Record (MBR) first	1 (1.3%)
– Victim ID and ransomware email	1 (1.3%)
– 2 encrypted files	1 (1.3%)
Total	***78 (100%)***

evaluated did not require any file or other type of additional resources. In other words, half of the decryptors would attempt to decrypt the compromised files without requiring the victim to supply any further data. On the other hand, 23 (30%) of the decryptors demanded a file in its original (plaintext) and encrypted form. These are requested to mount cryptanalytic brute-force attacks in an attempt to obtain the decryption key. The problem with this setting is that, after a successful attack, finding original copies of encrypted files could be particularly difficult for a significant number of victims, particularly those who do not have any backups. This requirement clearly shows that even having access to a ransomware decryptor for the concrete ransomware variant that compromised your system might not be enough to recover lost files and to reverse the harm done by the attack.

Additionally, 16 tools required extra resources. Typically, these resources are requested to find decryption key required to decrypt the encrypted files. For example, seven tools needed the ransom note, from which they could find the decryption key. Moreover, three decryptors requested a key file that the malware placed on the victim's computer to recover the master key used. An additional three decryptors necessitated for the decryption process to take place in the compromised machine and against the encrypted files created by the ransomware. Again, this provision was necessary so that the tool could locate the master keys or other essential resources to initiate the decryption of the lost files.

Lastly, Table 3 additionally shows that in some cases other uncommon info is needed, such as supplying a combination of the victim ID and the ransomware email, or having access to two encrypted files, or even performing a recovery of the Master Boot Record (MBR). In particular, the MBR recovery is necessary in the case of the Annabell ransomware, which locks the PC screen and then modifies the MBR. For this specific ransomware, the victim has first to clean up the infection and only afterwards use the decryption tool. On the other hand, both the victim ID and ransomware email combination, and the two encrypted files are needed to generate the decryption key for recovery.

5. Discussion

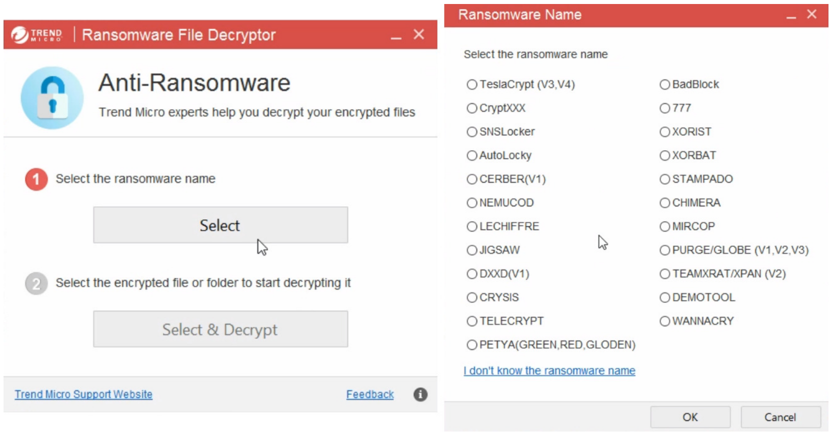
We evaluated the effectiveness of 78 decryption tools created by 11 security providers, listed on the No More Ransom website. Based on their performance, we divided these tools into three categories, as highlighted in table 2. We discuss those categories in detail below.

5.1. Full decryption

One thing that should be noted here is that the tools created by Emsisoft and Avast require victims to upload a plain and encrypted version of the same file. If the victims, as it will frequently be the case, lack access to the original file or a backup of it, they won't be able to recover their data. In contrast to Emsisoft and Avast, Bitdefender requires victims to upload just the encrypted file.

5.2. Partial Decryption

We placed one tool each from Bleeping Computer, Checkpoint/Cisco and Emsisoft into this category. That was because they could not decrypt all the ransomware strains they claim to support, or they could not recover the data completely.



TREND MICRO | Ransomware File Decryptor

Anti-Ransomware

Trend Micro experts help you decrypt your encrypted files

1 Select the ransomware name

Select

2 Select the encrypted file or folder to start decrypting it

Select & Decrypt

Trend Micro Support Website

Feedback

Ransomware Name

Select the ransomware name

○ TeslaCrypt (V3,V4)
○ CryptXXX
○ SNSLocker
○ AutoLocky
○ CERBER(V1)
○ NEMUCOD
○ LECHIFFRE
○ JIGSAW
○ DXXD(V1)
○ CRYSIS
○ TELECRYPT
○ PETYA(GREEN,RED,GLODEN)
○ BadBlock
○ 777
○ XORIST
○ XORBAT
○ STAMPADO
○ CHIMERA
○ MIRCOP
○ PURGE/GLOBE (V1,V2,V3)
○ TEAMXRAT/XPAN (V2)
○ DEMOTOOL
○ WANNACRY

I don't know the ransomware name

OK

Cancel

Figure 5: Trend Micro Decryptor supporting multiple ransomware strains

Please note that several companies – such as Trend Micro (see Figure 5 for the GUI of its tool) – have only one tool designed to decrypt multiple ransomware strains by choosing the right one from a list. Kaspersky has more decryptors, but the one we used during the testing was called “Rakhni Decryptor”. Bleeping Computer’s “desuCrypt” managed to decrypt one ransomware but could not crack another. Lastly, Checkpoint’s tool for the Jigsaw ransomware could only recover some files, not all.

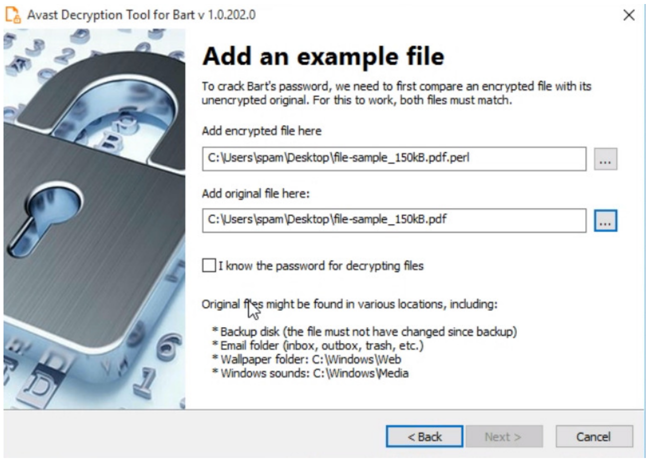
5.3. No Decryption

A surprising 41% of the tools did not recover any file encrypted by the ransomware they targeted.

These tools include seven by Avast, one by Bitdefender, three by Bleeping Computer, two by Cert, one by Checkpoint/Cisco, five by Emsisoft, six by Kaspersky, six by Trend Micro, and one by Tesorion.

As an example, the Avast decryption tool for the Bart ransomware required victims to enter a password to continue the recovery process (see Figure 6). This is the reason why Avast's tools did not work. The remaining tools did not detect the ransomware strain used in the test. It is possible that the attackers might have updated the ransomware binary after the tools were created.

Some of the decryptor download links were not working at the time of our investigation, such as the case with the Checkpoint/Cisco tool for the Derialock ransomware and the Police Nationale link for Pylocky. That is the reason why they were not included in our study. To decrypt files, Cisco requests PCAP (a network trace) files containing the outbound connection attempt by Pylocky. This is not realistic in most settings, as this info can be only caught seconds after the infection occurs[4]. Because of this unusual pre-requisite, we did not include it in the study.



Avast Decryption Tool for Bart v 1.0.202.0

Add an example file

To crack Bart's password, we need to first compare an encrypted file with its unencrypted original. For this to work, both files must match.

Add encrypted file here

C:\Users\spam\Desktop\file-sample_150kB.pdf.perl

Add original file here:

C:\Users\spam\Desktop\file-sample_150kB.pdf

□ I know the password for decrypting files

Original files might be found in various locations, including:

* Backup disk (the file must not have changed since backup)
* Email folder (inbox, outbox, trash, etc.)
* Wallpaper folder: C:\Windows\Web
* Windows sounds: C:\Windows\Media

Figure 6: Password required by Avast decryptor

[4] This is perfectly plausible for a well-managed system keeping traffic logs or a well-tuned network intrusion detection system, but this is hardly a common setting for infected machines.

5.4. Lessons Learned

All the tested tools were compatible across Windows 7 and Windows 10 operating systems. While many of these tools performed a good job at the recovery of the encrypted data, finding the correct tools may be troublesome. In order to hinder the decryption and removal process, some ransomware notes avoid revealing their names and mimic those of other strains, as in the case with TeslaCrypt V4.

No More Ransom has made decryption tools available for more than one hundred different types of ransomware. It also offers a detector called “Crypto Sheriff” that allows victims to upload encrypted files to identify the offending ransomware variant and provide them with the right available tools. We tested this tool by uploading the encrypted files and ransom notes corresponding to various ransomware families. While Crypto Sheriff detected some, many – such as Alcatraz, Avest, BigBobRoss, GandCrab, GetCrypt, Globe v3, Gomasom, InsaneCrypt, Noobcrypt, SpartCrypt and TeslaCryptV4 – were not properly classified. This is unfortunate, because the decryption tools for these ransomware strains are actually available on the No More Ransom website (and they work), but the Crypto Sheriff tool has severe trouble recognising them and pointing victims to the correct tool for recovery. Failing in their attempt to decrypt files may discourage victims from further efforts to restore their files, even though the decryptor for that ransomware may exist and work. Thus, a robust and more accurate ransomware detection and classification mechanism could make these tools significantly more usable and impactful to help victims.

6. Limitations and Future Work

The main limitation of our research is that we only managed to obtain 61 ransomware samples for which decryption tools were available. Although we searched for a total of 141 samples, we only found 72 ransomware binaries. Out of those, only 61 would execute. Likely, the 11 samples that did not run somehow – and despite our precautions – detected they were run in a VM environment.

Another possible reason for their behaviour was simply that their Command and Control (C&C) servers were not online any more.

For future work, we plan to explore two main research avenues. First, we want to expand our research by finding more ransomware samples to test the effectiveness of their associated decryption tools. We can also extend the testing across other operating systems, such as Linux and Android.

Additionally, we plan to use a walled garden notifications approach. Çetin et al. [27] highlighted that during their study, 27% of the users contacted their Internet Service Providers (ISPs) for additional help to remove malware from their system. Unfortunately, users lamented that they did not clearly understand the instructions provided by the ISPs. To overcome this problem, we can design a walled garden landing/notification page and ask the ISPs to use it for educating users after a ransomware infection. This page will raise awareness and could also help discourage victims from paying the ransom. This can be accomplished by highlighting that there is no guarantee they will get their files back even if they paid the ransom demand, as well as contributing to a better ransomware identification and by pointing to the right decryption tool, e.g. through leveraging the No More Ransom project more effectively.

7. Conclusion

In this paper, we present novel research on the effectiveness of ransomware decryption tools, i.e. how useful these tools really are at recovering victims' data.

We evaluated the effectiveness of 78 tools created by 11 security companies and investigated their features. The tools were tested against 61 different ransomware binaries. Only 55% of the examined tools managed to perform complete decryption of all encrypted files, 4% offered partial decryption, and a staggering 41% did not manage to decrypt any data. It is possible that attackers updated some of the ransomware strains tested and the encrypted files were no longer recoverable by these tools, but other issues may be at play as well.

The details of the tools that were not able to show any recovery capabilities have been shared with the relevant parties.

We also assessed the Crypto Sheriff's ransomware strain detection feature provided by the No More Ransom project. We conducted this evaluation by uploading encrypted files and ransom notes to examine whether they got correctly identified by Crypto Sheriff. Out of the 61 encrypted files and ransom notes uploaded, 43% (n = 26) were correctly identified, a troubling 49% (n = 30) were incorrectly identified and around a 8% (n = 5) were partially identified.

Our study suggests that existing tools are only capable of recovering victims' data for a small number of ransomware strains. Even when a decryption tool exists, chances are it will not be of much help in rescuing your data. That is why techniques and tools for the early detection of ransomware, such as Unveil and SheildFS, are extremely valuable. Despite that, the more decryption tools are known and used by victims, the greater the damage they would make on the cybercriminal's profits, because fewer victims would end up paying.

Through this paper, we wanted to highlight the relevance of these tools, but also to point out that improvements are direly needed in enhancing their accessibility and effectiveness. These decryption tools have a promising potential to make an important difference in combatting ransomware, and to hinder cybercriminal's operation as well as reducing their potential profits – and with them, disrupting the ransomware criminal business.

Acknowledgement

Part of the work presented in this paper was funded by the UK Engineering and Physical Sciences Research Council (EPSRC) Project EP/P011772/1 on the EconoMical, PsycHologicAl and Societal Impact of RanSomware (EMPHASIS).

References

[1] J. Pont, O. Oun, C. Brierley, B. Arief, and J. Hernandez-Castro, "A roadmap for improving the impact of anti-ransomware research," in *Nordic*

Conference on Secure IT Systems. Springer, 2019, pp. 137–154.

[2] G. O'Gorman and G. McDonald, *Ransomware: A growing menace.* Symantec Corporation, 2012.

[3] G. Hull, H. John, and B. Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses," *Crime Science*, vol. 8, no. 1, p. 2, 2019.

[4] A. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Communications of the ACM*, vol. 60, no. 7, pp. 24–26, 2017.

[5] K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware," in *Security Response.* Symantec, 2015.

[6] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention," 01 2017. [Online]. Available: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

[7] K. Zetter, "What Is Ransomware? A Guide to the Global Cyberattack's Scary Method," 2017. [Online]. Available: https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

[8] J. Hernandez-Castro, E. Cartwright, and A. Stepanova, "Economic analysis of ransomware," *Available at SSRN 2937641*, 2017.

[9] B. Groves, "Top 5 Cyber Threats to Businesses in 2019," 2019. [Online]. Available: https://www.cybergrx.com/resources/research-and-insights/blog/top-5-cyber-threats-for-businesses-in-2019

[10] S. Morgan, "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021," https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/, Oct. 2019.

[11] "No More Ransom." [Online]. Available: https://www.nomoreransom.org

[12] Europol, “No More Ransom: law enforcement and IT security companies join forces to fight ransomware.” [Online]. Available: https://bit.ly/2k2RCE8

[13] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions,” *Computers & Security*, vol. 74, pp. 144–166, 2018.

[14] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware,” in *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, 2016, pp. 757–772.

[15] N. Scaife, H. Carter, P. Traynor, and K. Butler, “Cryptolock (and drop it): stopping ransomware attacks on user data,” in *2016 IEEE 36th Int’l Conf. on Distributed Computing Systems (ICDCS)*, 2016, pp. 303–312.

[16] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, and F. Maggi, “ShieldFS: a self-healing, ransomware-aware filesystem,” in *Procs. 32nd Annual Conf. on Computer Security Applications*. ACM, 2016, pp. 336–347.

[17] N. Andronio, S. Zanero, and F. Maggi, “HelDroid: Dissecting and Detecting Mobile Ransomware,” in *Research in Attacks, Intrusions, and Defenses*, H. Bos, F. Monrose, and G. Blanc, Eds. Cham: Springer Int’l Publishing, 2015, pp. 382–404.

[18] D. Sittig and H. Singh, “A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks,” *Applied clinical informatics*, vol. 7, no. 02, pp. 624–632, 2016.

[19] S. Abraham and I. Chengalur-Smith, “An overview of social engineering malware: Trends, tactics, and implications,” *Technology in Society*, vol. 32, no. 3, pp. 183–196, 2010.

[20] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, 2007.

[21] L. Zhang-Kennedy, H. Assal, J. Rocheleau, R. Mohamed, K. Baig, and S. Chiasson, "The aftermath of a crypto-ransomware attack at a large academic institution," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1061–1078.

[22] F. Tang, B. Ma, J. Li, F. Zhang, J. Su, and J. Ma, "Ransomspector: An introspection-based approach to detect crypto ransomware," *Computers & Security*, vol. 97, p. 101997, 2020.

[23] Kaspersky, "The Cost of Cryptomalware: SMBs at Gunpoint." [Online]. Available: https://www.kaspersky.com/blog/cryptomalware-report-2016/5971/

[24] S. Mansfield-Devine, "Ransomware: taking businesses hostage," *Network Security*, vol. 2016, no. 10, pp. 8–17, 2016.

[25] E. Cartwright, J. Hernandez-Castro, and A. Cartwright, "To pay or not: game theoretic models of ransomware," *J. of Cybersecurity*, vol. 5, no. 1, p. tyz009, 2019.

[26] T. Meskauskas, *How to uninstall .google ransomware from the operating system*, 2020 (Last Accessed: October 16, 2020). [Online]. Available: https://www.pcrisk.com/removal-guides/17417-google-ransomware

[27] O. Çetin, C. Gañán, L. Altena, S. Tajalizadehkhoob, and M. van Eeten, "Let Me Out! Evaluating the Effectiveness of Quarantining Compromised Users in Walled Gardens," in *14th Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Aug. 2018, pp. 251–263.