An Investigation into the Effectiveness of Ransomware as a Method of Post-Exploitation Evidence Destruction

[Redacted]
Department of Cybersecurity and Computing
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

Context: In recent years ransomware has increased in prevalence significantly. With this, comes a more obscure variation of malware that masquerades as ransomware while providing no possibility of data recovery, dubbed "Wipers". These are used primarily as a method of destruction or concealment, possibly of extensive exploitative action, with motives far more significant than disruption or monetary benefit. This makes them distinct from traditional ransomware attacks in a number of ways.

Aim: The aim of this project is to evaluate the effectiveness of ransomware as a method of destroying evidence on a system after an attacker has obtained access by analyzing an infected device for information that may indicate the type or content of exploitation performed.

Method: A sample system will be set up and subsequently compromised, then infected with ransomware to mimic the behaviour of an attacker. Static and dynamic digital forensic techniques such as file carving and network monitoring will then be employed to assess if data related to the method of exploitation can be recovered post-infection.

Results: The project will assess what data can successfully be retrieved from an infected system (files, registry information, network connections) and to what extent aspects of exploitation can be successfully inferred, indicating either a success or failure to identify exploitative action post-infection.

Conclusion: This project will indicate the effectiveness of ransomware as a method of post-exploitation data destruction and thus provide context as to if and how attackers may employ it beyond the scope of traditional ransom demands.

Keywords

Ransomware; Digital Forensics; Data recovery; Data deletion; Post exploitation; Windows hacking

1. INTRODUCTION

Ransomware, malware that demands payment to retrieve data after encryption, has quickly become one of the most prevalent and common forms of malware employed – and undoubtedly the most disruptive. A number of the most significant of these attacks have been blamed on nation state attackers, such as WannaCry, believed to be North Korean in origin and most relevantly NotPetya, from Russia. Relative to independent Ransomware attacks, which are typically performed for monetary reasons, nation-states often employ ransomware as a method for disrupting or disabling critical infrastructure. To this end, a unique and more obscure variation of ransomware has arisen: coined “Wiper” ransomware or malware, owing to the fact it masquerades as ransomware due to its prevalence as a tool by traditional attackers; however notably, they offer no possibility of data recovery. This serves as a more effective solution wherein there is no motive nor desire for data recovery and serves to successfully waste defenders time by obscuring its true nature, giving false hope of data recovery.

Wiper malware is not typically considered to be the first choice for an attacker, as it would be logically more advantageous to obtain access to a system undetected and lurk but this malware is employable as an exit strategy if an attack is likely to be discovered and obfuscate details, or to grab and divert attention. Ukrainian authorities believed that NotPetya may have been a cover to install malware on the few machines that did not go offline during the attack for unclear reasons or to destroy past hacking evidence left by APT groups (Advanced Persistent Threats). (Polityuk & Auchard, 2017). Despite this relatively slim use case, the destructive potential of Wiper malware is unparalleled – with NotPetya still representing what is considered the most expensive and destructive malware attack in history, with the total cost being quoted as more than ten billion dollars in damages according to a senior white house official. (Greenberg, 2018)

Despite this: at present wiper ransomware has not seen widespread usage by individual attackers, largely because the scrutiny applied to attacks performed by individuals is far lower, and the stakes if they are discovered are lesser than a country – meaning obfuscation is less of a priority. However, techniques used by nation-states have typically trickled down to the average attacker with malware such as WannaCry now being easily accessible, and tools such as EternalBlue seeing widespread usage by individual groups. Given this, it is possible that ransomware-as-wiper may see increased usage in the event of major non-state cyberattacks in future, with wipers becoming more widely used by state actors recently. Therefore, assessing their validity as this form of tool when pitted against digital forensic analysis aids in identifying the risk of a competent attacker employing this as an effective form of data destruction, and possible remediations for a responder.

2. BACKGROUND

2.1 Ransomware

Ransomware is a form of malware characterized by the encryption of data alongside demands for money for its decryption. According to the National Cyber Security Center, Ransomware continues to represent one of the most acute cyber threats facing the UK in 2023 and beyond (NCSC, 2023). This has been evidenced by some of the most prolific and significant malware attacks of the past decade being performed with Ransomware, such as the infamous “WannaCry” attack of 2017 which served to cripple numerous

major organizations. The motive behind these attacks varies, with it ranging from monetary benefit in the case of individual groups or disrupting significant infrastructure to send a political message in the case of nations.

Within this, ransomware as a type has several varieties of malware that it encompasses, with examples such as the most common: Locker ransomware; which prevents access to a system wholly, or Crypto ransomware; which allow access but still encrypt all files. This means that ransomware attacks can require a significantly different methodological response depending on the infection.

2.2 "Wiper" malware

Wiper malware is malware characterized by its operation as erasing or wiping data, typically the entire drive, of the system it infects. One of the earliest examples of this form of malware was "Shamoon" deployed by Iran against the Saudi Oil company, Saudi Aramco in 2012 (Dehlawi & Abokhodair, 2013)which quickly established wipers as a valid cyber weapon between enemy states. Since this, most instances of major wiper attacks have arrived in the form of geopolitical cyberattacks. The most significant of these attacks came in the form of NotPetya in 2017 which targeted Ukraine, with approximately 75% of all infections (Lika, et al., 2018) being localized to the area.

NotPetya was noteworthy for pretending to be a variant of the Petya ransomware, going as far as to imply data recovery was possible despite subsequent analysis indicating that there was no chance of recovery due to code changes from the standard Petya ransomware preventing the production of a valid decryption key (Lika, et al., 2018). This represented a development, in that wipers typically did not attempt to masquerade as other forms of software in the past. Since then, this has become more common – with wiper ransomware variants such as "WhisperGate" and "Somnia" arriving in the form of similarly faux ransomware. This has increased significantly in the past 5 years, mainly targeting Ukraine in the Ukraine/Russia conflict, with wipers several new variants such as HermeticWiper and AcidRain being employed. (See figure 1).

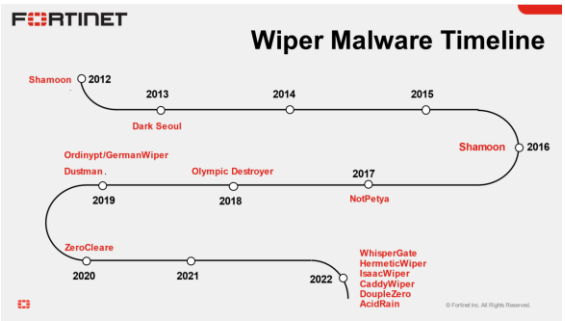

Figure 1 – A timeline of "Wiper" malware (Revay, 2022)

2.3 Digital forensics

Digital Forensics relates to the examination and recovery of data stored digitally. This can be performed in a variety of ways, such as analyzing network traffic or file carving, the process of reassembling files from what they leave behind after deletion/corruption. This is typically performed through two means: Static and dynamic. Static relates to performing analysis on files, or an inactive system, often a storage drive. Dynamic analysis requires a system to be active while collecting data, which is then analyzed, this encompasses most network or memory data.

For ransomware, digital forensics typically relates to the field of data recovery through drive analysis. However, research has shown that modern decryption tools provided by security companies to recover files after ransomware, while effective, still have significant improvements to be made given that 41% failed to decrypt any files on a victim's system when tested (Filiz, et al., 2021) which points to the effectiveness of ransomware at preventing access to a system despite forensic analysis.

As such, even when data recovery is possible (as in the case of ransomware, where data recovery is theoretically intended) retrieval is a significant struggle post-infection, meaning that ransomware serves as an ideal scapegoat for wiper malware given the outcome may be identical if a ransom is not paid. Due to this, data collection prior to infection hosted elsewhere, such as network monitoring, is essential for a digital forensic investigation wherein ransomware has the potential to be employed.

However, recent research has shown the effectiveness of open-source digital forensics tools. For example, Autopsy, a Graphical Interface for The Sleuth Kit, a widely employed suite of digital forensics tools has been indicated to have some success. Research performed showed that against the ransomware WannaCry, Autopsy could be used effectively to recover all data from an infected Windows 11 computer including elements such as browser search history (Nayak, et al., 2023). This suggests that ransomware data recovery may be possible using readily accessible tools, including data indicating exploitation.

3. METHOD

3.1 System setup

Prior to the introduction of ransomware, a victim system must be set up. This will be a Windows machine, most likely Windows 10 as it is the most common variation of Windows installed worldwide currently and thus the most likely to see attack, making it most representative. This will be set up to mimic an individual PC on a network with some monitoring, attempting to simulate a small government organization or business which are those mainly targeted by this form of malware historically. It will have low security in place (excluding that necessary for malware detonation) such as a medium/low complexity password and thus represent a valid target for a potential malicious attacker.

In order to ensure the reproducibility and consistency of the results, this will be hosted as a virtual machine through VMware Workstation with snapshots taken prior to infection and reloaded should malware need to be detonated again. This system will not be connected to the internet though will be connected to an internal network, featuring another system used for monitoring. No malware analysis tools will be installed on this system such that no detection code is tripped within the ransomware in order to ensure that it best emulates a standard system.

3.2 System hacking

In an attempt to best identify what behavior can be spotted, a number of different exploitative actions will be performed on the system to provide a sample of those that an attacker may

do, these will include: Running malicious scripts, registry modification, leaving files behind, password cracking attempts, external SSH connections (To a theoretical control server) and accessing malicious sites which in turn should give a broad scope for detection, and indicate which of these actions can be successfully identified post-infection.

3.3 Malware

To assess the various types of ransomware that may be employed, three different strains representing three different forms of ransomware will be detonated:

- Crypto ransomware - Ransomware that encrypts files but still allows for login and basic functions.
- Locker ransomware – Typical ransomware that locks function until a ransom is paid.
- Wiper "ransomware" – Ransomware designed to wipe and destroy, not payable, with no chance of file decryption.

This is such that they can be compared in terms of effectiveness as a tool for an attacker, and validity of data recovery for a defender. These will be detonated on the victim system.

3.4 Forensic tools

To effectively simulate a monitored network, dynamic analysis will be performed by having a second machine on the same network as the victim machine prior to infection during exploitation and post-infection. This will be monitoring network traffic fulfilling the role of an IDS (Intrusion detection system) or other similar network monitoring that would typically be employed in a small government or business organization. Memory analysis using tools such as Volatility will not be employed, as this is unrealistic in a typical environment and is unlikely to be monitored. Static analysis will be primarily performed by using the infected system (if it is accessible, as in the case of Crypto ransomware) post exploitation to assess what functionality is still available and if information can be identified from it, related to registry access, command line history etc. Subsequently, static analysis will be performed through tools such as Autopsy to analyze the drive and other file carving tools may be employed such as Foremost to see if elements such as files or registry information can be identified.

3.5 Risk assessment

The most critical risk associated with this project is the risk of malware infection of the testing PC. While numerous efforts will be taken to ensure the safe detonation of malware, with the strain chosen not known to be able to escape virtual machines – any time malware is used on a system, infection is a possibility. This would, at worst, destroy the testing computer and require it to be reimaged as it would not be connected to any other systems on the network so spread is minimized. Other risks include technical failure of the main virtual machine in so far as not booting, which is somewhat likely though would be easily fixable – as setting up a new Windows 10 virtual machine is of low complexity. Given the broad scope of the project, it is not unreasonable that failure to complete the project within the given timeframe may occur – though with appropriate management (Such as the usage of Gantt charts) this should be mitigated to a manageable extent.

4. Summary

This project highlights the risk that arises with ransomware proliferation as it becomes an increasingly accessible tool for attackers, with it representing an easy method of evidence destruction. The results will indicate the viability of investigation if a hack is suspected and ransomware is deployed, as well as the most effective types of ransomware for evidence destruction which indicates those most likely to be used by attackers for this purpose. This would be of primary benefit to a post-exploitation investigator as it would allow for assessment as to whether ransomware was likely used as an obfuscatory measure based on type, and the viability of subsequent analysis.

5. REFERENCES

Dehlawi, Z. & Abokhodair, N., 2013. *Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident.* Seattle, IEEE.

Filiz, B., Arief, B., Cetin, O. & Hernandez-Castro, J., 2021. On the Effectiveness of Ransomware Decryption Tools. *Computers & Security,* Volume 111.

Greenberg, A., 2018. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* [Online] Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 10 October 2024].

Lika, R. A., Murugiah, D., Brohi, S. N. & Ramasamy, D., 2018. *NotPetya: Cyber Attack Prevention through Awareness via Gamification.* Shah Alam, Malaysia, IEEE.

Nayak, S. C., Tiwari, V. & Samanthula, B. K., 2023. *Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform.* Las Vegas, IEEE.

NCSC, 2023. *NCSC Annual Review 2023.* [Online] Available at: https://www.ncsc.gov.uk/pdfs/reports/Annual_Review_2023.pdf [Accessed 7 October 2024].

Polityuk, P. & Auchard, E., 2017. *Global cyber attack likely cover for malware installation in Ukraine: police official.* [Online] Available at: https://www.reuters.com/article/us-cyber-attack-ukraine/global-cyber-attack-likely-cover-for-malware-installation-in-ukraine-police-official-idUSKBN19K1WI/ [Accessed 7 October 2024].

Revay, G., 2022. *An Overview of the Increasing Wiper Malware Threat.* [Online] Available at: https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat [Accessed 7 October 2024].