# The Ransomware Epidemic: Uncovering the True Costs and Impacts on Individuals and Businesses

Branden Barnes

CYSE 280: Windows System Management and Security

Professor Gladden

December 7, 2023

## Abstract

Ransomware remains a heightened vector of cyber-attacks around the world. They possess the ability to dismantle vast regions of critical infrastructure. This halt, dischargeable by malware, can wield immense economic downfall. Understanding the functionality of ransomware drafts the initial step in the mitigation process. If and when malware appears, how well response teams intercept and uncover defining factors of the code, will ensue an expounding moment of loss prevention. Learning from attacks will be key in upgrading system patches. These updates will increase the likely hood of protection from following consecutive attacks. What can be done about ransomware attacks is our ability to learn and redefine strategic advancements for the betterment of system improvement.

## Overview

June 27, 2017, pronounced the first notified precedent of a Petya malware variant. Petya ransomware, also known as "NotPetya," is a Microsoft Windows operating system malware known for its encryption of files within a system, and furthermore nestling its way into the Master Boot Record (MBR). Using a hard-coded list, Petya ransomware gains administrative rights that deem infected Windows computers inoperative. It then can spread quickly through the victim's files, latching itself further through the infected system using a backdoor (Petya Ransomware: CISA, 2023).

[1] Propagation methods used by NotPetya:

- PsExec - a legitimate Windows administration tool

[1] (Petya Ransomware: CISA, 2023)

- WMI - Windows Management Instrumentation, a legitimate Windows component
- EternalBlue - the same Windows SMBv1 exploit used by WannaCry
- EternalRomance - another Windows SMBv1 exploit

[2]An official report released from the Nation Cybersecurity and Communications Integration Center (NCCIC) states NotPetya incorporates one distinctive file, "this file is a dynamic-link library (DLL) designed to appear as ransomware, but which is, in effect, a data wiper. During runtime, this application attempts to steal victim's credentials and use them to spread laterally on a compromised network. The malware also utilizes the EternalBlue Server Message Block (SMB) exploit for lateral movement." The encryption process consists of a vigorously generated 128-bit key on the Master File Table (MFT) of the victim's hard drive.

## WannaCry Ransomware

May 2017, WannaCry ransomware was launched. This ransomware package included a worm, which allowed it to snake amongst compromised systems. WannaCry targeted outdated Microsoft Windows computers with a crypto ransomware package. When exploited, the victim's computer would show a request for bitcoin in exchange for privilege to their files. However, this ransomware was not programmed with the ability to decrypt files, so if ransom was paid, files were still lost. Similar propagation techniques as NotPetya were used. EternalBlue was the exploit that allowed access and DoublePulsar was used as the backdoor.

[3]The National Cybersecurity and Communications Integration Center (NCCIC) reported how the WannaCry infects host computers. "It attempts to exploit vulnerabilities in the Windows SMBv1

[2] https://www.cisa.gov/sites/default/files/publications/MIFR-10130295.pdf

[3]https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

server to remotely compromise systems, encrypt files, and spread to other hosts. Systems that have installed the MS17-010 patch are not vulnerable to the exploits used." When reverse-engineered, a kill switch was found in the URL domain. This URL was registered and dispersed worldwide, putting a stop to further spread of this version of WannaCry ransomware.

## Methodology

NotPetya and WannaCry ransomware infected hundreds of thousands of systems in over 150 different countries. Economic disparities were estimated in the billions of dollars amongst large corporations and individuals. In order to prepare against ransomware, it is important to understand the ransomware life cycle (Silva, López, Caraguay, Álvarez, 2019).

[4] The ransomware life cycle can be described in seven steps, as follows:

1. Ransomware design

2. Ransomware dissemination

3. Ransomware arrival

4. Command and Control communication (C&C)

5. Search user's information

6. Encryption

7. Extortion and financial claiming

---

[4] (Silva, López, Caraguay, Álvarez, 2019).

Developing ransomware packages can involve unique modifications, but the process follows the ransomware lifecycle beginning with design and ending with extortion. Typical variations include a filecoder, which encodes files, and lockscreen, which disables computer access (Silva, López, Caraguay, Álvarez, 2019). The formulator can design their new version of ransomware based off popular development kits, "(Torlocker, TOX, or Hidden Tear)." Availability of malware kits make it easy for non-skilled attackers to create ransomware code. Once created, the next step for the developer is to decide on a means of dissemination. There are several different ways of spreading malware; "phishing or spam e-mails, exploit kits (malvertising), downloader and trojan botnets, social engineering tactics, traffic distribution systems (TDS), among others" (Silva, López, Caraguay, Álvarez, 2019). Inside these vectors contain a way of inserting ransomware en route toward victim files. Encryption process begins once inside, locking the user out and hosting financial claiming for the return of files.

## Frameworks

Wade and Seek framework is a hostage negotiation tactic when files are being held at ransom. This framework consists of five stages. Stage one, acknowledge that the hacker is technically skilled. Letting the hacker know their infiltration hasn't gone unnoticed but instead credited may give a rapport for a more auspicious net result. "Wading ever so slightly into the psyche of the hacker will allow victims to seek out a more favorable outcome. This is also a mitigation strategy for escalation, particularly if the entity attacked denies the attack publicly" (Wade, 2021). Stage two, "play the victim" (Wade, 2021). The hacker may feel incline to empathy resulting in a potential lowering of ransom. Stage three, follow trails of released files from the attacker. "This shows the attacker is willing to gain the hostage's trust and is therefore more interested in a quick payout. An attacker may also extend the deadline, showing they are willing to be flexible on their

end for some payout, if not the full amount" (Wade, 2021). Stage four, create leverage. Stage five, use all interactions with the attacker in hopes that the negotiation will allow you to retrieve your data.

## Tools

Antivirus companies are working hard to continually put out greater mitigation techniques and updates to servers. The best way to stay safe from ransomware attacks is to follow their guidelines. Malware continues to upgrade, finding more vulnerabilities to code every day. To stay one step ahead, review Anti-malware techniques available and be sure to allow for patches to run their course. When WannaCry was rampaging through filesystems, antivirus companies were able to expand on their updates, saving millions from falling to variants of ransomware once again. Effectively safeguarding end-user devices is crucial for the security of IT systems "(workstations, mobile devices), regardless of the platform, as a significant part of serious security incidents stem from a user device (patient zero)" (Szücs, V., Arányi, G., & Dávid, &, 2021).

[5]Antivirus solutions known for supporting large manufacturers:

- Real-time download and email (anti-spam and anti-phishing) control module,
- Multi-layered ransomware protection with behavior-based learning ability,
- Sandboxing,
- WEB content and URL filtering,

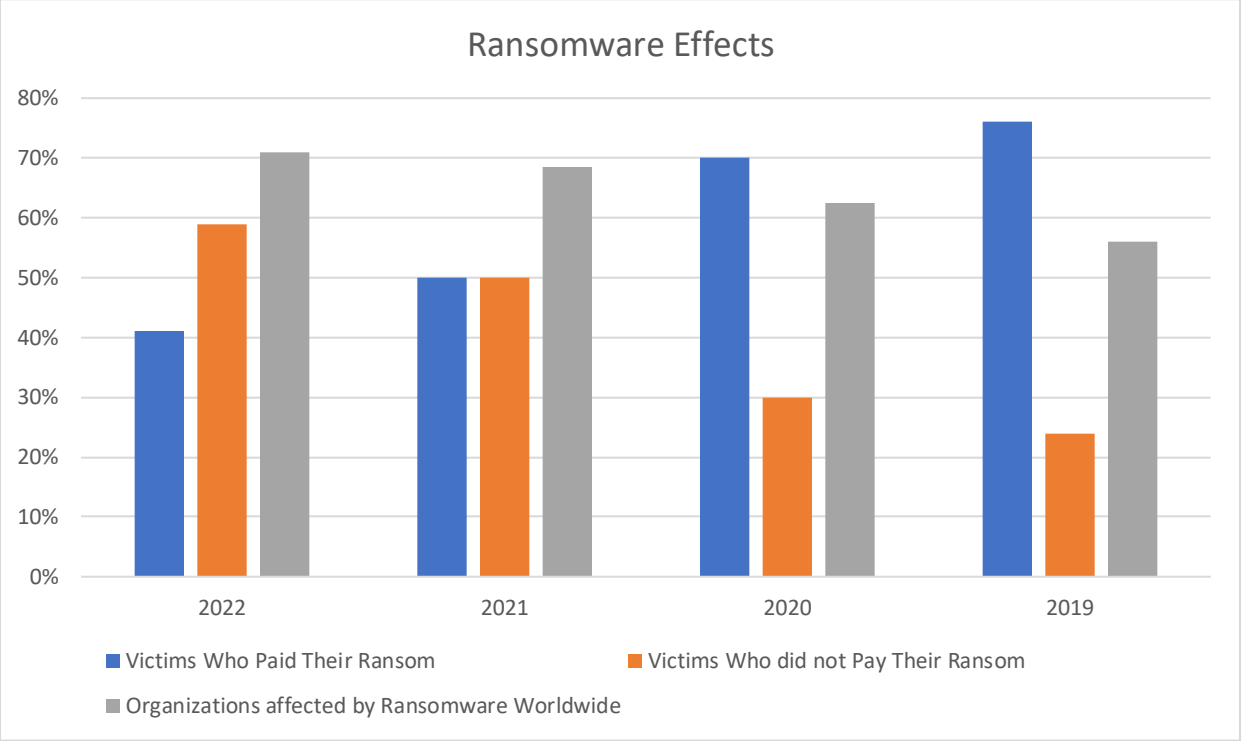
[5] (Szücs, V., Arányi, G., & Dávid, &, 2021).

- Proprietory software firewall,
- Proprietory VPN service,
- Secure DNS service,
- Webcam protection,
- Custom file and directory access layer,
- Network vulnerability analysis,

Only some protection examples are listed above. With those examples, additional protection techniques are run simultaneously. Effectively countering extortion viruses necessitates actions such as monitoring lateral movement within the network, overseeing operations on centralized storage, implementing efficient logging practices, and establishing appropriate automatic backup systems (Szücs, V., Arányi, G., & Dávid, &, 2021).

## Conclusion

Institutions should follow guidelines when preventing ransomware attacks. It is more prominent now then it was in earlier years how destructive ransomware can be. It is important within an organization to have teams regularly monitoring malware vulnerabilities, as well as, testing employees on their knowledge for determining what is and what isn't a risk for malware. From the data I have observed, the understanding of ransomware is increasing along with awareness. No company wants a breach in their security. Frameworks should be pronounced. A companies cybersecurity policy should leave room in their cost benefit analysis for ransomware attacks. Overall, benefits of having a ransomware readiness program allows for companies to seek out their vulnerabilities and understand their risks.


Ransomware Effects
80%
70%
60%
50%
40%
30%
20%
10%
0%
2022
2021
2020
2019
Victims Who Paid Their Ransom
Victims Who did not Pay Their Ransom
Organizations affected by Ransomware Worldwide

## References

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons, 64*(6), 787-797.

*Petya Ransomware: CISA*. Cybersecurity and Infrastructure Security Agency CISA. (2023, December 7). https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

Herrera Silva, J., Barona López, L., Valdivieso Caraguay, &., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sensing (Basel, Switzerland), 11*(10), 1168.

Szücs, V., Arányi, G., & Dávid, &. (2021). Introduction of the ARDS—Anti-Ransomware Defense System Model—Based on the Systematic Review of Worldwide Ransomware Attacks. *Applied Sciences, 11*(13), 6070.

Jai Vijayan, C. W. (2023, October 17). *Ransomware profits decline as victims dig in, refuse to pay*. Ransomware Profits Decline as Victims Dig In, Refuse to Pay. https://www.darkreading.com/cyberattacks-data-breaches/ransomware-profits-decline-victims-refuse-pay

Ani Petrosyan, & 1, S. (2023, September 1). *Global users attacked by Ransomware trojans 2022*. Statista. https://www.statista.com/statistics/1410098/cyber-crime-users-targeted-ransomware-trojans-number-monthly/