WHITE PAPER

An Empirically Comparative Analysis of Ransomware Binaries

By Shannon Davis

splunk>
turn data into doing

Executive Summary

Security researchers and network defenders have written many words on ransomware, yet many organizations continue to react tactically to such attacks rather than with mindful intent. This is due in part to the lack of ground truth knowledge about ransomware. Ransomware encryption speed is one area that merits further study. To date, the most comprehensive information on this subject comes from the LockBit ransomware authors themselves, who provide a comparison of ransomware family encryption speeds on their website to advertise that they are the "fastest." This paper aims to illuminate an area of study that was previously left to criminals. Utilizing the scientific method in a controlled environment, we measured the speed at which 10 variants of popular ransomware malware encrypted nearly 100,000 files, totalling nearly 53GB, across different Windows operating systems and hardware specifications. Through this work, we hope to give defenders more knowledge and confidence to move "left of boom" with their detections rather than waiting to detect during the "actions on objective" phase that is discussed in the Lockheed Martin Cyber Kill Chain whitepaper.

To determine the speed of ransomware encryption, we created a modified version of the Splunk Attack Range lab environment to execute 10 samples of each of the 10 ransomware variants on four hosts. Two hosts ran the operating system Windows 10 and the other two hosts ran Windows Server 2019. We chose to attribute the ransomware samples to each variant by only selecting samples confirmed by Microsoft Defender Antivirus in VirusTotal. We assigned each host "high" or "mid" level resources to test how ransomware would behave with different processors, memory, and hard drive configurations. We enabled Windows logging on each host to collect, synthesize, and analyze the data in Splunk. This allowed us to measure how fast the ransomware variants encrypted nearly 100,000 files, and how the ransomware utilized system resources like processor, memory and disk.

After running all one hundred ransomware samples, we determined the total time to encrypt (TTE) varied from four minutes to three and a half hours with a median speed of 42 minutes. This narrow timeline provides a limited window for organizations to effectively respond before encryption is complete. When comparing identical ransomware strains across systems with different resources, we found some variables could impact TTE, such as processor speeds or CPU cores. However, the impact was inconsistent, implying that some ransomware was single-threaded or minimally able to take advantage of additional resources. LockBit ransomware was the fastest variant to encrypt on any system. This aligns with previous reports that LockBit only encrypts 4KB of each file, rendering the file unusable and expediting the attack. The title of "fastest ransomware" also matches the LockBit developer's own public claims on the group's Tor website.

SURGe plans to build upon this research to create a comprehensive, high-level overview of ransomware for network defenders. In particular, we plan to review the file access techniques of multiple ransomware samples using open-source file analysis framework tools like stoQ, fuzzy algorithms, and Splunk's Machine Learning Toolkit (MLTK). Furthermore, we plan to investigate claims that modern ransomware is not masked with packers and determine if it is possible to cluster to-be-determined classifiers of unknown ransomware binaries as they are "deployed" rather than detect them after execution. We plan to release the dataset for this research at .conf22 in June of 2022. We encourage researchers to investigate this corpus and validate or build upon our findings to help the global community of blue teamers.

Key Findings

- LockBit ransomware performed the fastest out of 10 ransomware variants in our testing, which aligns with the ransomware group's claims on their Tor site
- The median time for ransomware variants to encrypt across a corpus of 98,561 files measuring 53.83 GB, was 42 minutes and 52 seconds.
- Individual ransomware samples varied greatly in encryption speed, ranging from four minutes to three and a half hours.
- Improved hardware capabilities provided some ransomware samples with faster encryption speeds. Other samples and variants were unable to take advantage of the increased resources, and at times they performed worse on the systems with higher specifications. Additional memory did not have a significant effect on encryption speed for any of the samples. Higher disk speeds may play a role in faster execution, but most likely in combination with a variant that can take advantage of additional CPU cores.

Introduction

In the 2021 M-Trends report, Mandiant found that 25% of their investigations in 2020 involved ransomware, up from 14% in 2019.[1] The Verizon Data Breach Investigations Report (DBIR) of 2021 states that ransomware doubled in frequency from 2019 to 2021.[2] Although relatively new in the public consciousness, this style of malware has afflicted the world since it was first introduced at an AIDS conference in 1989 via floppy disks.[3]

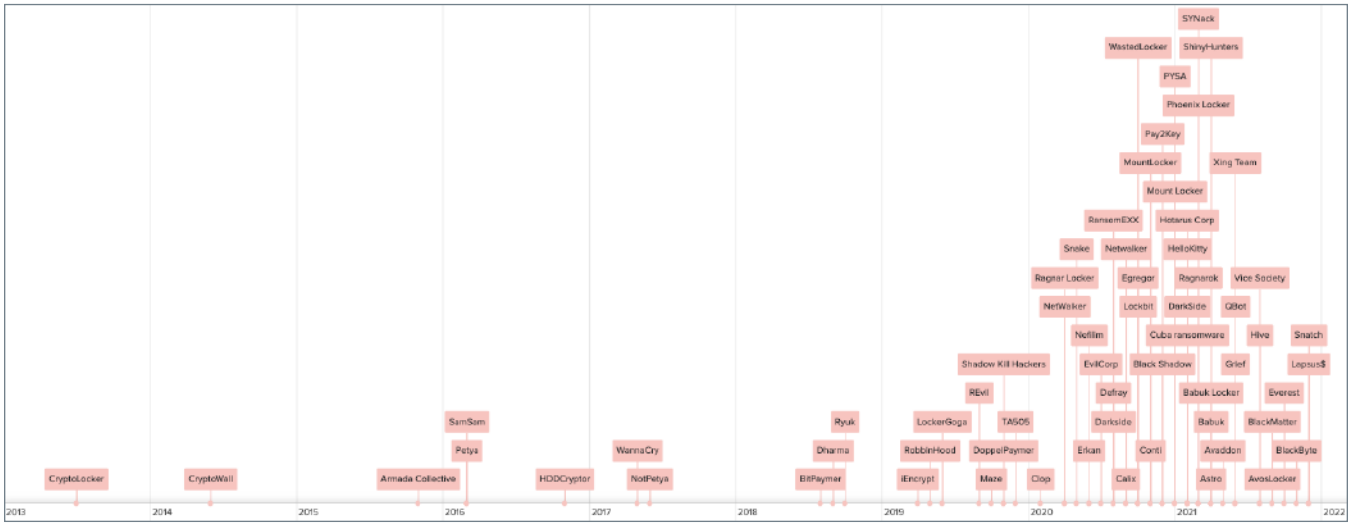

Figure 1. Spunk chart highlighting the growth of ransomware families from 2013 to 2022.

The previously mentioned M-Trends report states that in the Americas, ransomware has a median dwell time of three days.[4] A dwell time of three days does not sound ideal, but there is a long-held perception that ransomware has a shorter dwell time of mere hours or even minutes. If the median dwell time is measured in days and not hours, defenders have a small window of opportunity to take action. In 2021, CERT NZ published a whitepaper that outlines the lifecycle of ransomware with recommendations to help organizations combat this growing threat (fig. 2).[5]

1. FireEye and Mandiant, "Fireeye-Rpt-Mtrends-2021.Pdf," April 13, 2021, 13, https://www.mandiant.com/resources/m-trends-2021.
2. Verizon, "DBIR 2021 Data Breach Investigations Report," May 12, 2021, 14, verizon.com/dbir.
3. "Case Study: AIDS Trojan Ransomware," SDxCentral, accessed February 23, 2022, https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/.
4. FireEye and Mandiant, "M-Trends 2021," 14.
5. "How Ransomware Happens and How to Stop It," CERT NZ, accessed January 29, 2022, https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/.

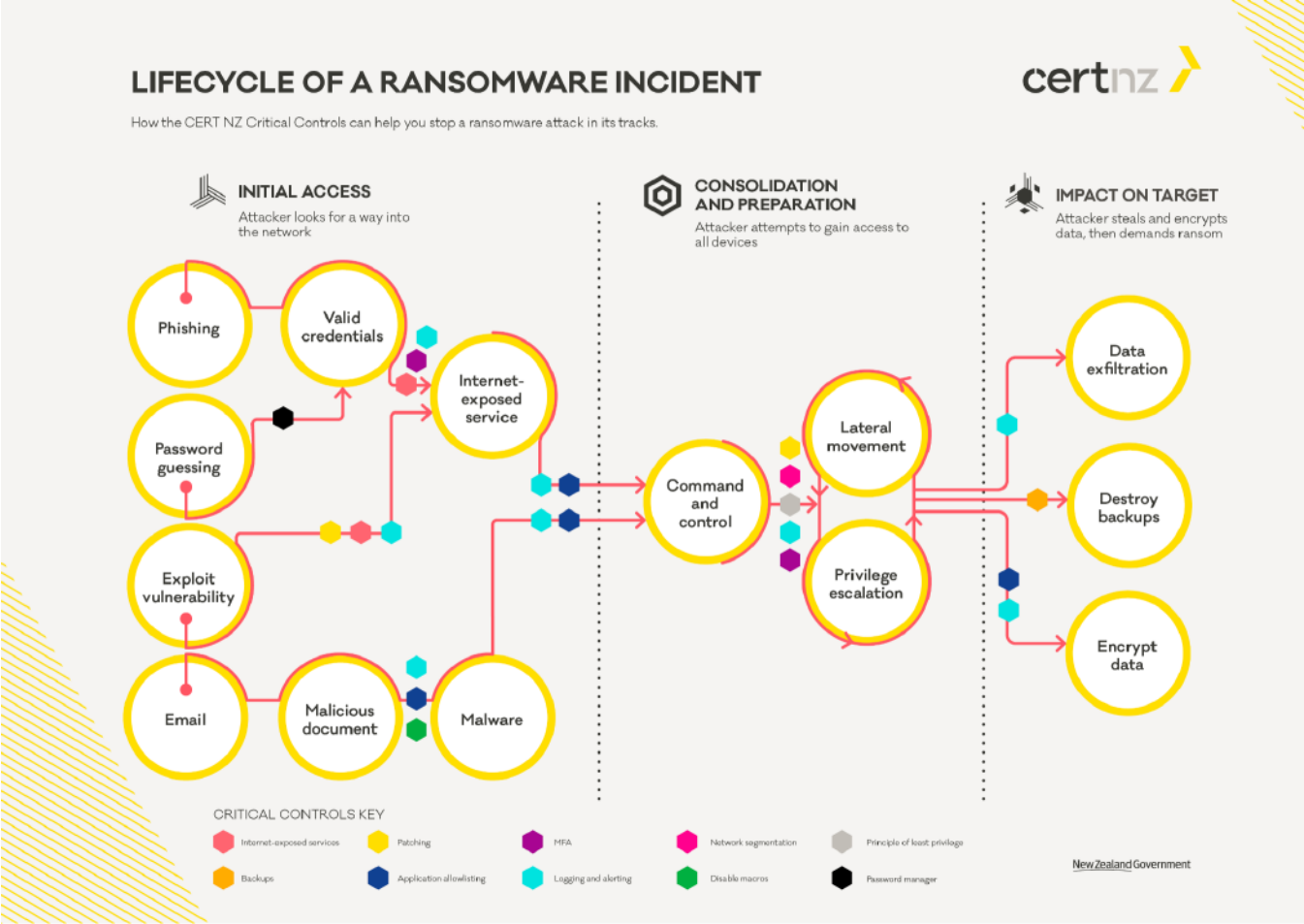

Figure 2. Detailed progression of a ransomware incident from CERT NZ.

This work by CERT NZ and the three-day dwell time cited by Mandiant led us to question how organizations can actively defend against ransomware. Before we began looking at defensive methodologies, we decided to first investigate two questions:

- Primarily, how long do ransomware strains take to encrypt a host?
- Can an organization recover or prevent the complete encryption of file systems?

Reverse engineers have done great work to learn why some ransomware strains are so fast to encrypt. With the exception of an advertisement from the Lockbit ransomware group, we were unable to find any empirical study that compares the speed of encryption among different ransomware families.[6,7] This paper outlines our analysis of the dynamically evaluated encryption speed for 10 ransomware families and provides some suggestions for blue teamers to better inform their defenses. It should be noted that this paper does not aim to create ransomware detections. Rather, our objective is to inform defenders of the holistic truth of ransomware encryption speeds.

“This paper outlines our analysis of the dynamically evaluated encryption speed for 10 ransomware families and provides some suggestions for blue teamers to better inform their defenses.”

6. “LockBit BLOG,” accessed February 13, 2022, http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion.ly/conditions.
7. Gridinsoft LLC, “LockBit Ransomware. The Most Honest and the Fastest,” Gridinsoft LLC, accessed January 29, 2022, https://gridinsoft.com.

Setting the Stage

We started to brainstorm our hypothesis with unbounded questions about how fast ransomware encrypts and how organizations can move "left of boom" if the ransomware encrypts quicker than expected.[8] We began by synthesizing our questions to a single hypothesis: **If an adversary gains access to a system and deploys ransomware, then encryption will occur faster than network defenders can realistically prevent**. The Verizon DBIR states that the majority of organizations detect breaches days after an adversary gains access to a system, rather than hours or minutes.[9] To test our hypothesis, we needed to create a lab for repeated testing, gather samples of different ransomware binaries, and then analyze our findings. We also desired to conduct this research in a manner that catered to blue teamers. Thus, we chose not to perform static reverse engineering work on the malware binaries, but instead executed them dynamically in a controlled environment and measured them against the same variables. We plan to include a detailed explanation of our methodology and technical process in future blogs, papers, and conference presentations.

In this section of the whitepaper, we explain how we framed our experiment to test our hypothesis. We also detail the high-level architecture, configuration of our malware lab, and how and why we sourced our malware. Finally, we set out any known assumptions in our research and analysis that may present bias in our findings.

Methodology

To test our hypothesis, we needed to execute a variety of ransomware strains in a controlled environment, gather native Windows performance telemetry data back from endpoint hosts, and analyze the data. We selected 10 ransomware families with 10 separate binaries from each of those families in order to prevent clustering illusion, the tendency to see patterns where none exist, and confirmation bias, the tendency to seek out information that supports one's beliefs. For each Windows endpoint type and resource specification, a single Amazon Web Services (AWS) Virtual Private Cloud (VPC) was created for each family and each individual binary ran on its own host specifically created for its evaluation. The results were forwarded to a central Splunk instance for analysis. Every host had 98,561 files placed in 100 directories. These file types were sourced from the Digital Corpora and deemed by the authors to be the most likely file types for ransomware binaries to encrypt.[10,11,12] These files were made available under the CC0 license and sourced from public U.S. government websites. Finally, we enabled Event ID 4663 on Windows hosts in order to see encryption on files and baseline the speed of each ransomware family.[13]

8. John McHale, "Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems," accessed January 30, 2022, http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom.
9. Verizon, "DBIR 2021 Data Breach Investigations Report," 90.
10. Simson Garfinkel et al., "Bringing Science to Digital Forensics with Standardized Forensic Corpora," Digital Investigation 6 (September 2009): S2–11, https://doi.org/10.1016/j.diin.2009.06.016.
11. "Digital Corpora Downloads: Corpora/Files/Govdocs1/By_type/," accessed January 30, 2022, https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/.
12. "Digital Corpora Downloads: Corpora/Files/Govdocs1/Zipfiles/," accessed January 30, 2022, https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/.
13. Microsoft, "4663(S) An Attempt Was Made to Access an Object. (Windows 10) - Windows Security," accessed January 30, 2022, https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663.

The Lab

As previously mentioned, the research was conducted against ransomware binaries executed in a controlled environment. The performance of the ransomware was gathered using native Windows auditing and logging capabilities that forwarded the results back to a Splunk instance. Details on the telemetry setup are covered in more detail in the Experiment Procedure section. Each ransomware sample ran inside an independent, self-contained environment. The Splunk instance in each ransomware environment forwarded the events to a single Splunk instance for comparing, analyzing, and reporting. We created the lab by modifying Splunk's open-source Attack Range tool for our experiment (fig. 3).[14] Attack Range allows network defenders to dynamically create small networks in AWS with Splunk software and logging preconfigured using a combination of Terraform and Ansible.

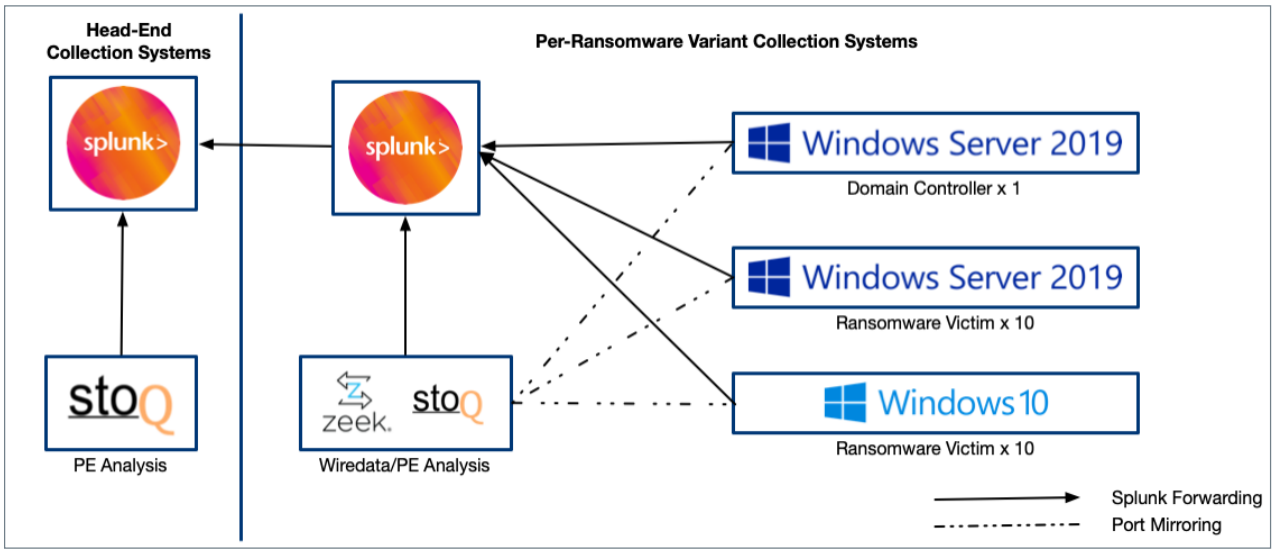

Figure 3. A high-level overview of our custom Attack Range.

The hosts on this range had specifications that aligned with many modern laptop or server builds according to organizations that we gathered anecdotal feedback from and popular websites like PC Mag.[15] These hosts had Microsoft Defender uninstalled, and no additional anti-virus (AV) or endpoint detection and response (EDR) tools installed. We installed additional tools including a Splunk agent to send information back to Splunk and the Microsoft application Sysmon.[16] Finally, to detect any worming or remote mapped file encryption, these hosts were joined to a Windows domain with an open network share (C Drive) on the domain controller. More information about the host specifications and the logging configurations can be found in the appendices A and B. In order to capture file encryption events, we enabled object level auditing on the test directory and all sub-directories for both successful and failed access attempts. By enabling object level auditing, Event Code 4663 events were generated each time the ransomware binary attempted to encrypt a file. The final 4663 event to conclude a successful encryption of a file was DELETE, which is what we used to track encryption speed. While this event was seen consistently across the families we tested, this DELETE event may not be present in other families. If this is the case, a different marker might be needed to measure TTE.

14. Splunk Attack Range, Jinja (2019; repr., Splunk GitHub, 2022), https://github.com/splunk/attack_range.
15. "Dell Latitude 7420 Review | PCMag," accessed January 30, 2022, https://www.pcmag.com/reviews/dell-latitude-7420.
16. markruss, "Sysmon - Windows Sysinternals," accessed February 25, 2022, https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

Experiment Procedure

To best emulate modern ransomware campaigns, we executed the ransomware across 10 Windows 10 hosts and 10 Windows Server 2019 hosts via a remote PowerShell script located on the Windows Server 2019 Domain Controller. This remote PowerShell method was used to initiate the ransomware infection as opposed to a user having to manually execute the binary. This methodology had the added benefit of emulating modern ransomware campaigns where ransomware is executed by human operators via scripts rather than by victims on desktops. Furthermore, it reduced some overhead of "human interaction," which allowed the ransomware to utilize more system resources than would have otherwise been available. We did not pass any flags to the ransomware when it executed. The only ransomware variant that we executed in a different manner was Babuk, as it would not run reliably using the remote PowerShell method, and we therefore started Babuk interactively on each host. Two different hardware profiles for each operating system were used to evaluate ransomware performance. The exact specifications for these profiles can be found in Appendix B.

The PowerShell script allowed us to select the ransomware sample we wanted to run. The script would then iterate through the number of Windows 10 or Windows Server 2019 hosts in the domain and initiate downloads of the ransomware binaries via a remote web server. Each test run was either on a Windows 10 or Windows Server host, never both at the same time.

When the download finished on each host, the PowerShell script launched each ransomware binary remotely, except for Babuk. We were then able to analyze the speed that each variant encrypted files using Windows security event logs. Event Code 4663 (an attempt was made to access an object) was required to capture the encryption events reliably. We enabled file system auditing for the 100 test directories on the Windows 10 and Windows Server 2019 hosts in order to generate the required event logs.

The Ransomware Binaries

The 100 ransomware samples across 10- ransomware families were sourced from VirusTotal. We solely leveraged Microsoft Defender detections from VirusTotal for ransomware family attribution. The ransomware families were selected due to their prevalence over the past 12 to 24 months (fig. 4).

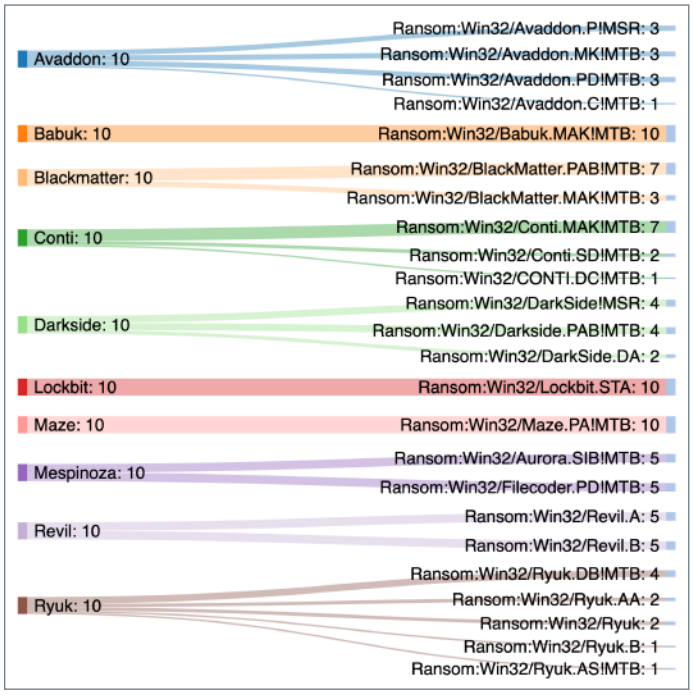

Figure 4. The 10 ransomware families and their respective strains were selected for our research.

The VirusTotal detection strings and SHA256 hashes of each binary tested in each family can be found in Appendix C.

Results

The answer to our initial question of how fast ransomware encrypts showed a large variance between ransomware families. We wanted to understand the encryption speed and duration for each sample as well as the median speed and duration across the families themselves. Using the median value as opposed to the average/mean value prevented small numbers of outliers from skewing the overall results of a particular family.

As we collected Windows Perfmon data during our testing, we observed that some families utilized increased system resources better than others. Some of the families were very efficient, while others tended to utilize large percentages of CPU time along with very high disk access rates. There was no direct correlation between a sample using a larger amount of system resources with a faster encryption speed. Some ransomware families performed worse, or even crashed, when deployed on the faster test systems.

On a per sample basis, the fastest encryption time across the 98,561 test files observed was 4 minutes and 9 seconds. This was performed by lockbit-9.exe (133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0) on a Windows 2019 Server high specification instance (fig. 5).

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09	396

Figure 5. Data from the lockbit-9.exe sample deployed on a Windows 2019 server.

Conversely, the slowest encryption time observed for the same test file set was 3 hours, 35 minutes and 8 seconds. This was performed by babuk-5.exe (1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02) on a Windows 10 mid specification instance (fig. 6).

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Babuk	Win-10-Mid	C:\ransom\babuk-5.exe	03:35:08	8

Figure 6. Data from the babuk-5.exe sample deployed on a Windows 10 instance.

When we look at the median encryption duration across each family tested we found that although a single sample of Babuk was the slowest ransomware to encrypt, the Babuk family as a whole was the second fastest with a duration of 6 minutes and 34 seconds. LockBit was still the fastest overall at 5 minutes and 50 seconds. The slowest median encryption time per family was Mespinoza, (PYSA) with a median duration time of 1 hour, 54 minutes, and 54 seconds. Overall, the median encryption duration across all ransomware families was 42 minutes and 52 seconds (fig. 7).

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
Average of the median	**00:42:52**

Figure 7. Median encryption duration across 10 ransomware families.

The average median duration demonstrates a limited window of time to respond to a ransomware attack once the encryption process is underway. This can prove even more limiting considering that the catastrophic apex may be when a single critical file is encrypted, rather than the whole of the victim's data. With such factors in play, it may prove to be extremely difficult, if not impossible, for the majority of organizations to mitigate a ransomware attack once the encryption process begins. While detection and defensive capabilities are beyond the scope of this research, all is not lost for those looking to defend themselves against ransomware attacks.

We took care to ensure our methodology for capturing this data didn't influence the outcome of the data we collected. However, we were limited in our ability to measure the latency that these tools, such as Sysmon and constrained Object Level Auditing, may have introduced. We don't believe these tools caused any significant latency that would drastically alter the findings in our research. Future research that focuses on ransomware encryption speeds may wish to ensure that there is a means of measuring the latency that tooling may introduce. Finally, we recognize that the attribution of ransomware samples to "families'' can be difficult. In order to ensure consistent bias of sample selection for this research, we compared the hashes of each sample with Microsoft Defender results obtained from VirusTotal. The signature name was extracted and then normalized. We then used the resulting normalized value to identify the specific ransomware family.

Conclusions and Further Work

The goal of this research was to empirically evaluate the encryption speed of common ransomware families across a variety of operating systems and hardware specifications in order to determine if organizations could realistically react in time for effective mitigation. Based on our median results, our findings indicated a total loss of data via ransomware encryption occurs in under 43 minutes. The encryption and loss of data is the "actions on objective" of the formerly mentioned Lockheed Martin Cyber Kill Chain. Forty-three minutes is an extremely limited window of opportunity for mitigation, especially considering that the average time to detect compromise is three days, as the Mandiant M-Trends report found. As a result, we postulate that it's unlikely many organizations can prevent a total loss of data from ransomware. If an organization wishes to defend against ransomware, it's clear that they need to move left on the cyber kill chain and detect on delivery or exploitation rather than actions on objective. We are hopeful that findings from this research can help network defenders better explore and identify potential opportunities for mitigation. It should also be noted that although we configured our lab to detect wormable behavior by the ransomware samples, the majority of samples had no such behavior. Future research will explore worming behavior in further depth.

Our research does not stop with this work. We plan to release this corpus of information on the Splunk BOSS Platform to enable additional areas of research that warrant exploration. More specifically, we hope to evaluate the patterns that ransomware exhibits when encrypting files, ransomware worming behavior, how to cluster similar ransomware binaries based on fuzzy hashing algorithms, and future analysis of ransomware family attribution over time.

Acknowledgments

Research like this takes more than just the primary and secondary investigators to create. A special thanks to Allie Mellen, Mark Harris, David French, Ryan Kovar, Audra Streetman, Marcus LaFerrera, Mick Baccio, Dave Herrald, Drew Church, Johan Bjerke, John Stoner, Tamara Chacon, Kelcie Bourne, Scott Roberts, Adam Swanda, Michael Haag, and the authors of the Splunk Attack Range from the Splunk Threat Research Team (STRT).

Bibliography

- SDxCentral. "Case Study: AIDS Trojan Ransomware." Accessed February 23, 2022. https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/.
- "Dell Latitude 7420 Review | PCMag." Accessed January 30, 2022. https://www.pcmag.com/reviews/dell-latitude-7420.
- "Digital Corpora Downloads: Corpora/Files/Govdocs1/By_type/." Accessed January 30, 2022. https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/.
- "Digital Corpora Downloads: Corpora/Files/Govdocs1/Zipfiles/." Accessed January 30, 2022. https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/.
- FireEye, and Mandiant. "Fireeye-Rpt-Mtrends-2021.Pdf," April 13, 2021. https://www.mandiant.com/resources/m-trends-2021.
- Garfinkel, Simson, Paul Farrell, Vassil Roussev, and George Dinolt. "Bringing Science to Digital Forensics with Standardized Forensic Corpora." Digital Investigation 6 (September 2009): S2–11. https://doi.org/10.1016/j.diin.2009.06.016.
- CERT NZ. "How Ransomware Happens and How to Stop It." Accessed January 29, 2022. https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/.
- LLC, Gridinsoft. "LockBit Ransomware. The Most Honest and the Fastest." Gridinsoft LLC. Accessed January 29, 2022. https://gridinsoft.com.
- "LockBit BLOG." Accessed February 13, 2022. http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion[.]ly/conditions.
- markruss. "Sysmon - Windows Sysinternals." Accessed February 25, 2022. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.
- McHale, John. "Defending DoD from Cyberattacks, Getting to the Left of the Boom - Military Embedded Systems." Accessed January 30, 2022. http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom.
- Microsoft. "4663(S) An Attempt Was Made to Access an Object. (Windows 10) - Windows Security." Accessed January 30, 2022. https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663.
- Microsoft Security Intelligence. "Trojan:PowerShell/Redearps.A Threat Description," March 24, 2021. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:PowerShell/Redearps.A&threatId=-2147189091.
- Splunk Attack Range. Jinja. 2019. Reprint, Splunk GitHub, 2022. https://github.com/splunk/attack_range.
- Symantec. "THE INCREASED USE OF POWERSHELL IN ATTACKS." Symantec Corporation, 2016. https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en.
- Verizon. "DBIR 2021 Data Breach Investigations Report," May 12, 2021. verizon.com/dbir.

Appendix A: Windows Logging Configuration

- Windows file system auditing (Event Code 4633) enabled on C:\Files\ and all subdirectories (directories 0-99). This was enabled for both failed and successful attempts at modifying a file.
- Windows process creation (Event Code 4688) with command-line logging enabled
- Sysmon installed and configured with a verbose configuration from Olaf Hartong

Appendix B: Host Specs

- Win-10-High- Windows 10, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD (3000 IOPS/125MBs throughput)
- Win-10-Mid- Windows 10, AWS m5.xlarge (4 CPU/16GB RAM) 300GB HDD (3000 IOPS/125MBs throughput)
- Server-2019-High- Windows Server 2019, AWS m5.4xlarge (16 CPU/64GB RAM) 300GB HDD (10000 IOPS/500MBs throughput)
- Server-2019-Mid- Windows Server 2019, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD (3000 IOPS/125MBs throughput)

Appendix C: Ransomware families and binaries

Binary	SHA256 Hash	VirusTotal Vendor	VirusTotal Detection
avaddon-0.exe	078de7d019f5f1e546aa29af7123643b-d250341af71506e6256dfee8f245a2a7	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-1.exe	18c1ad49bf46b44df5926851ca30f00f6675c-535b6826a3c779099643327ea33	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-2.exe	288165763637cda27304d90bb7ec47e103dfb69fd-f6c009d113b1f6852c091a0	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-3.exe	3a040105b3cb704c838a87061dba6b-03712d308636a438004300ec154de2d4d6	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-4.exe	4adc6cac6071cd67773c9cefab479f0ffde370c4ce-dac31b6db4de065c3ec7af	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-5.exe	572610a5033a2060afa67ddbfd7345013e82c6904d-d7ace22cb6f0b0bedcb550	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-6.exe	743079700007b64647d9ea4a0c361e6e981518ed-06a5902ab9f275c38aa45c7b	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-7.exe	b9e62cb99e71c856cc41edfd837689993b7fc-63c780e5786c34b2a8f63ef37b6	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-8.exe	cc95a8d100f70d0fbf4af14e852aa108bdb0e36db-4054c3f60b3515818a71f46	microsoft	Ransom:Win32/Avaddon.C!MTB
avaddon-9.exe	d8acd139f4f99b3137ab4cea9ef9e515e3a-560f25a79666ac302f21d468340f8	microsoft	Ransom:Win32/Avaddon.PD!MTB
babuk-0.exe	04126b30c1c2663cdf2b6386781aedbfce2ef418a0b-01de510bd536903f577e3	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-1.exe	049e53f72c8afa5ccb850429d55a00e2f-be799e68247fd13f5058146cf0f4cf8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-2.exe	106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-3.exe	12c561ac827c3f79afff026b0b1d3ddec7c-4b591946e2b794a4d00c423b1c8f8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-4.exe	1b04e1fbddfcdb16a3d103e50261937815668d-92d4909a15352dd5e2615adbf4	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-5.exe	1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff-8c17032aa017f6075c02	microsoft	Ransom:Win32/Babuk.MAK!MTB

Binary	SHA256 Hash	VirusTotal Vendor	VirusTotal Detection
babuk-6.exe	1f37064ff61211d7a0d0428af856323bafb734b3f8b0e-44d04e8e0db872349ee	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-7.exe	245e191bfe998ad9ef2d6b169af22f-3c290e9950234f8ddd0f4a03cb3eebf761	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-8.exe	2509e5a4535d25110663a698410847aa0cb-9ce734722076ada4c651532f318a5	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-9.exe	25835a890a218fd26bfd8b23696576402b5eb8a4c9a-f4a51529e14c4f00a9cce	microsoft	Ransom:Win32/Babuk.MAK!MTB
blackmatter-0.exe	8eada5114fbbc73b7d648b38623f-c206367c94c0e76cb3b395a33ea8859d2952	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-1.exe	26a7146fbed74a17e-9f2f18145063de07cc103ce53c75c8d-79bbc5560235c345	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-2.exe	2aad85dbd4c79bd21c6218892552d-5c9fb216293a251559ba59d45d56a01437c	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-3.exe	496cd9b6b6b96d6e781ab011d1d02ac3fc3532c8bdd-07cae5d43286da6e4838d	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-4.exe	b4b9fdf30c017af1a8a3375218e43073117690a71c-3f00ac5f6361993471e5e7	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-5.exe	6d4712df42ad0982041ef0e2e-109ab5718b43830f2966bd9207a7fac3af883db	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-6.exe	be5bc29f58b868f4ff8cd66b4526535593e-515a697bb8951c625bdfed13cccb7	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-7.exe	ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f-526c1fe3b8bf2d6e7404	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-8.exe	7a223a0aa0f88e84a68da6cde7f7f-5c3bb2890049b0bf3269230d87d2b027296	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-9.exe	9bae897c19f237c22b6bdc024df27455e739be24be-d07ef0d409f2df87eeda58	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
conti-0.exe	004ede55a972e10d9a21bcf338b4907d6eed65bf5ad-6abbbd5aec7d8484bdedf	microsoft	Ransom:Win32/Conti.SD!MTB
conti-1.exe	17ac91a36237d8f37dcee961ba74c9310a45c009780ea-092c3a1e428870ff8a1	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-2.exe	34366c9a9ac34dd9016abd406cffe-713a3e8606e8600e6cb07e0242904f91a5b	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-3.exe	49dc5a243d322cd4d467e5f24b61ff749869564ddc-f6a2f700839cf5ae9e37ea	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-4.exe	0b0b902af452e1c949a609a3b29a9de21dac639846c77427de06e6e63c1fe904	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-5.exe	73bd8c2aa71f5dcd9d2ddd79e53656c6ae3d-b2535e08cf9dab1cd13bdd6d5ea3	microsoft	Ransom:Win32/CONTI.DC!MTB
conti-6.exe	8df9b346bf591629a9eb0bf9f-32c545a1266873495ceec9ba990be1dd22b9aa9	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-7.exe	0ffbc914e3bb09df586a93e5a5a557d03c5fcce7e8ee-4a36bd3a09b8ed429c7a	microsoft	Ransom:Win32/Conti.SD!MTB
conti-8.exe	d43b52e3453ce77d2694a239232f39341a-98fa704954a558125e74a85f22a346	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-9.exe	1201e76d42f85feb89d64e6fd497144ed3afe-66281b2464e84f3b889f2867c9b	microsoft	Ransom:Win32/Conti.MAK!MTB
darkside-0.exe	22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6	microsoft	Ransom:Win32/DarkSide!MSR

Binary	SHA256 Hash	VirusTotal Vendor	VirusTotal Detection
darkside-1.exe	2c323453e959257c7aa86dc180bb3aaaa5c5ec-06fa4e72b632d9e4b817052009	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-2.exe	45ecce9dfec886e2b092a996f6affb9e7417d6121e-58b0ec643be7e36a03106d	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-3.exe	7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b-85896fc4b431990a5984	microsoft	Ransom:Win32/DarkSide!MSR
darkside-4.exe	84af3f15701d259f3729d83beb15ca738028432c261353d1f9242469d791714f	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-5.exe	c6e2ef30a86baa670590bd21acf5b91822117e0c-be6060060bc5fe0182dace99	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-6.exe	2c1e20a4b38634b97de398246bc3c8082d-47663702a46bb885dc7fcc5f71daa1	microsoft	Ransom:Win32/DarkSide!MSR
darkside-7.exe	43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdf-ce1a896db17a374eb8aa	microsoft	Ransom:Win32/DarkSide!MSR
darkside-8.exe	533672da9d276012ebab3ce9f4cd09a7f537f-65c6e4b63d43f0c1697e2f5e48d	microsoft	Ransom:Win32/DarkSide.DA
darkside-9.exe	5da3e6b4bea1eaceddb048a4a6bd702291189f42d-15c4b2670de78984329b0a9	microsoft	Ransom:Win32/DarkSide.DA
lockbit-0.exe	00ad914476509f84b40f2dbe804dc-7c37a1a24ef3472674574d3367079bf0a2a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-1.exe	04f65270c92dda82c759c1eee49cf8f-4c98a2ed0071272e49132331fda482dba	microsoft	Ransom:Win32/Lockbit.STA
lockbit-2.exe	082f91d85c437f415cea44b36afb4198da07b-78593c836a398cd96365166e7d8	microsoft	Ransom:Win32/Lockbit.STA
lockbit-3.exe	50d08c974f7abce-2da5c2a8976d3c6017334a418359d7bb031bd0914b-848b24a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-4.exe	0cd33e6b180862072a00a0c2f897afa754df071bc-ec3d13e581c41a5c27a3102	microsoft	Ransom:Win32/Lockbit.STA
lockbit-5.exe	7a1fb0eac9b62ce510030f9ff983d9d6225fd8dad6f-05c1051c335aca87ffa24	microsoft	Ransom:Win32/Lockbit.STA
lockbit-6.exe	0d4966b4724f141adb7a7db1d9ae48f5c293c6049cc7f-949220256c2e72ab5ac	microsoft	Ransom:Win32/Lockbit.STA
lockbit-7.exe	bb736c8d3dd2b3ebcacd3e2a61f95b-20d23bc981cc22888dff88cfd2e720ee99	microsoft	Ransom:Win32/Lockbit.STA
lockbit-8.exe	d68cad561a949648a84ffc2f2db186f585cd4a90951e-ea91c1c100d996cb3688	microsoft	Ransom:Win32/Lockbit.STA
lockbit-9.exe	133adb408a4837d3a20634d79baf-01151061c49cd936e9a8787b91df8997b6b0	microsoft	Ransom:Win32/Lockbit.STA
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d-669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d-669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-1.exe	0b9c99276ed36110afc58b3fb59a-da135146180189c25d99618ca5897537ee21	microsoft	Ransom:Win32/Maze.PA!MTB
maze-2.exe	2a6c602769ac15bd837f9ff390acc443d023ee62f76e1be8236dd2dd957eef3d	microsoft	Ransom:Win32/Maze.PA!MTB
maze-3.exe	b3473d205ba722e229f49002093b61fc35902e-1a67bcd558bf9a7811278e5cb2	microsoft	Ransom:Win32/Maze.PA!MTB
maze-4.exe	5a06ae8540d5a0d7fb88e80d3e61c3a6079f3abdafe-998ce70ffdcac9e940520	microsoft	Ransom:Win32/Maze.PA!MTB

Binary	SHA256 Hash	VirusTotal Vendor	VirusTotal Detection
maze-5.exe	877c439da147bab8e2c32f03814e3973c22cbcd-112d35bc2735b803ac9113da1	microsoft	Ransom:Win32/Maze.PA!MTB
maze-6.exe	9d86beb9d4b07dec9db6a692362ac3fce-2275065194a3bda739fe1d1f4d9afc7	microsoft	Ransom:Win32/Maze.PA!MTB
maze-8.exe	e45eacf5158bb2aa11f29f0675b4cb68dbf7e-376569516fe33f84be524c67763	microsoft	Ransom:Win32/Maze.PA!MTB
maze-9.exe	ecd04ebbb3df053ce4efa2b73912fd4d086d1720f-9b410235ee9c1e529ea52a2	microsoft	Ransom:Win32/Maze.PA!MTB
mespinoza-0.exe	0433efd9ba06378eb6eae864c85aafc8b-6de79ef6512345294e9e379cc054c3d	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-1.exe	0f0014669bc10a7d87472cafc-05301c66516857607b920ddeb3039f4cb8f0a50	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-2.exe	164cb8e82d7e07cca0409925cadd8be5e3e8e07d-b88526ff7fe87596c6a6bd07	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-3.exe	4dc802894c45ec4d119d002a7569be6c99a9b-ba732d0057364da9350f9d3659b	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-4.exe	1e2009549452ed-6b524b94ed683079ee60c2b9542b1bfd-5b9ee42e9161d5e7c8	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-5.exe	327934c4c11ba37f42a91e1b7b956d5a4511f918e63047a8c4aa081fd39de6d9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-6.exe	425945a93beb160f101d51de36363d1e7ebc-45279987c3eaf5e7f183ed0a3776	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-7.exe	44f1def68aef34687bfacf3668e56873f9d603fc6741d-5da1209cc55bdc6f1f9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-8.exe	4770a0447ebc83a36e590da8d01ff4a418d-58221c1f44d21f433aaf18fad5a99	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-9.exe	48355bd2a57d92e017bdada911a-4b31aa7225c0b12231c9cbda6717616abaea3	microsoft	Ransom:Win32/Filecoder.PD!MTB
revil-0.exe	d74cd044351030290f6ad8f70f91d51b6c39675ca3c-70c45b5b0c5bd09589ff6	microsoft	Ransom:Win32/Revil.A
revil-1.exe	338e8f24eeb38b5ef67ef662b65d592c816eba94d-faaac856021dac407daf294	microsoft	Ransom:Win32/Revil.A
revil-2.exe	ab53e6823e47b446a245374c7760006ee84c8ea45 7a5fe9ca9df4732bf55a32a	microsoft	Ransom:Win32/Revil.A
revil-3.exe	73dd3cb487dfb863304d9f6d79f60b2ab4adbd162e-460a2210b4a6abf049ea53	microsoft	Ransom:Win32/Revil.B
revil-4.exe	151271bf05310f94cd33cba3eb90be264edc-4828c04e4e82f492b8e2576ee7a6	microsoft	Ransom:Win32/Revil.B
revil-5.exe	97f905bb24c5054d09fe79a20e04fe84042ad985b-5c6e09afad21efa83dcd7a0	microsoft	Ransom:Win32/Revil.A
revil-6.exe	19f1a30555b83f23acc245ef6fe745f3292ef015c71a-bef8daa077e31f259179	microsoft	Ransom:Win32/Revil.B
revil-7.exe	1f7b15f6cf07c5943ce8ab5bfd0700e4919808f-ca4260ffd2a509100d45fadaf	microsoft	Ransom:Win32/Revil.B
revil-8.exe	1fb842e87f23e37ab39e201a024845c323c3d-239331768db694dca96ed53d8c7	microsoft	Ransom:Win32/Revil.B
revil-9.exe	21bcb9c0095424a179399379939f6ebdf1dfe202825c-1ca5acdd25a8f751402f	microsoft	Ransom:Win32/Revil.A
ryuk-0.exe	487d4698c6c938ca3e9251827a5813ddd21e26584b-3459d768e457ddd4e8c4d4	microsoft	Ransom:Win32/Ryuk.DB!MTB

Binary	SHA256 Hash	VirusTotal Vendor	VirusTotal Detection
ryuk-1.exe	4cb0bf61d61ad3383636df11b3e4da8e67bb0ace-a03e981ecdd48d08ed8c796c	microsoft	Ransom:Win32/Ryuk.AA
ryuk-2.exe	dea1b54618643ffe59506398f0f131300abe0988da-89b5414955843ae5b53fee	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-3.exe	0cf36731f5b8651d53fc651607c3fc-cac24b631c08dca4493d8e07d2fbff1db3	microsoft	Ransom:Win32/Ryuk.AA
ryuk-4.exe	8027a5e9dfcb379592868fb61fd8ed5f1605f0e4460d-b53d23a859d2a9743b91	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-5.exe	d4b8cbfa94bac3dbd58452fcc6c4e0b-56b65a54a671a2184d9fb6e3694a0266f	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-6.exe	ba595e53ea6b0ef7f3332c2fec6a644c3cbc9756d-2978c49e69eba92526904d8	microsoft	Ransom:Win32/Ryuk.B
ryuk-7.exe	fc4d44faf906e7a6ba133dae5f33ce22b8569943574ff-ccadd0292b12abcc8fa	microsoft	Ransom:Win32/Ryuk.AS!MTB
ryuk-8.exe	fe55650d8b1b78d5cdb4ad94c0d7ba-7052351630be9e8c273cc135ad3fa81a75	microsoft	Ransom:Win32/Ryuk
ryuk-9.exe	568d73074880063d4d2b3e9d3ddb-938685de8ec8e24974ff32f5f47d55a2dcb0	microsoft	Ransom:Win32/Ryuk

Appendix D: Encryptable File Type Corpus

Extension	Count	Total Size (MB)
html	25364	1,589.66
pdf	25185	15,116.11
txt	14856	12,632.61
doc	7955	5,019.95
jpg	7095	1,020.12
ppt	5576	11,044.64
xls	4238	4,384.81
gif	2010	114.83
ps	1186	2,024.57
csv	1005	224.24
xml	918	137.19
gz	794	435.43
log	514	622.12
unk	433	63.2
png	317	19.12
text	184	136.18
dbase3	170	3.03
f	129	14.11
rtf	128	31.35
eps	67	14.23
pps	65	164.05
swf	43	20.41
wp	42	4.2
fits	39	58.58
tex	36	2.25

Extension	Count	Total Size (MB)
java	36	1.24
kml	32	4.03
kmz	28	2
pptx	21	75.78
troff	21	1.9
bmp	13	5.23
docx	13	0.85
sgml	9	0.22
sql	7	0.46
hlp	7	0.02
dwf	5	0.56
gls	5	0.02
tmp	4	0.9
data	2	0.77
NO EXTENSION	1	124.94
zip	1	0.84
vrml	1	0.32
wk1	1	0.31
py	1	0.23
ttf	1	0.12
g3	1	0.12
xlsx	1	0.05
pub	1	0.000049
	98,561 Files	**53.83 GB Total**

Appendix E: Endpoint Performance Findings

Windows Server 2019 High Specification

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-High	95.52	96.18	61.64	628.67	67.62	8	167890.42	54246.70	55118.46	17.28	227.62	26.13
Babuk	Server-2019-High	34.82	99.74	99.36	452.19	67.89	8	3853.88	28099.74	26860.70	25.72	178.65	19.27
Blackmatter	Server-2019-High	8.25	11.90	5.47	313.81	35.74	10	1962.33	10263.18	10283.99	12.70	117.03	16.99
Conti	Server-2019-High	6.88	12.97	8.59	257.58	18.58	8	343.72	11532.70	11492.30	164.83	237.50	17.46
Darkside	Server-2019-High	6.94	21.29	16.21	311.21	35.54	10	1670.40	8721.45	8731.53	12.00	113.81	16.41
Lockbit	Server-2019-High	27.02	41.55	15.94	502.12	28.07	8	1531.18	1237.26	1399.21	7.79	110.66	19.06
Maze	Server-2019-High	4.29	5.88	4.40	365.64	3.38	8	2086.59	13216.13	4831.49	4.19	86.45	16.28
Mespinoza	Server-2019-High	5.76	7.54	4.97	153.03	2.03	8	64.42	8191.90	6142.31	3.48	47.67	8.07
Revil	Server-2019-High	7.06	18.38	13.29	243.36	35.16	8	2425.00	14108.76	14068.99	11.61	105.26	15.01
Ryuk	Server-2019-High	53.31	86.33	20.02	171279.74	53.82	8	2931.32	62045.03	82201.84	181.45	296.14	102.16

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-High	43868	7.58	5787.00	53.9
Babuk	Server-2019-High	98560	5.55	17760.00	166
Blackmatter	Server-2019-High	98553	37.41	2635	24.55
Conti	Server-2019-High	98560	64.07	1538	14.34
Darkside	Server-2019-High	98553	43.60	2260	21.07
Lockbit	Server-2019-High	98548	5.30	18622	173
Maze	Server-2019-High	98560	86.53	1139	10.62
Mespinoza	Server-2019-High	97080	102.55	946.70	8.824
Revil	Server-2019-High	98553	27.25	3618	33.71
Ryuk	Server-2019-High	89521	8.92	9266	93.6

Windows Server 2019 Mid Specification

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-Mid	95.42	97.16	51.46	467.96	35.69	8	166866.12	44362.49	45706.62	14.84	140.11	23.97
Babuk	Server-2019-Mid	29.07	160.58	147.78	380.75	36.21	8	2985.14	21796.16	20907.03	17.95	133.61	16.87
Blackmatter	Server-2019-Mid	7.40	9.33	4.55	313.49	19.62	10	1688.89	8863.80	8850.98	11.45	95.38	16.49
Conti	Server-2019-Mid	7.10	12.33	7.93	241.00	10.41	8	117.35	10851.88	10881.95	83.15	145.91	16.57
Darkside	Server-2019-Mid	6.23	18.67	14.12	332.28	19.48	10	1495.22	7732.50	7725.44	10.86	95.34	16.22
Lockbit	Server-2019-Mid	22.40	33.26	13.45	458.79	18.10	8	1205.07	975.23	1092.23	7.02	96.55	18.76
Maze	Server-2019-Mid	4.02	4.94	3.95	333.54	4.46	8	1572.07	10751.79	3887.37	3.46	68.76	13.73
Mespinoza	Server-2019-Mid	5.39	6.70	4.65	153.03	2.02	8	80.30	6782.18	5023.70	3.55	47.27	8.11
Revil	Server-2019-Mid	6.62	17.54	12.86	254.25	19.30	8	2147.04	12687.87	12605.01	11.11	86.37	15.27
Ryuk	Server-2019-Mid	41.19	59.49	14.45	218856.14	53.61	8	1965.13	38545.07	56935.97	182.73	300.70	102.88

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-Mid	50307	8.75	5749.00	53.6
Babuk	Server-2019-Mid	98560	6.51	15140.00	141
Blackmatter	Server-2019-Mid	98553	43.18	2283	21.27
Conti	Server-2019-Mid	98560	67.60	1458	13.59
Darkside	Server-2019-Mid	98553	50.47	1953	18.20
Lockbit	Server-2019-Mid	98548	6.76	14594	136
Maze	Server-2019-Mid	98560	114.75	858.94	8.006
Mespinoza	Server-2019-Mid	97080	124.55	779.48	7.265
Revil	Server-2019-Mid	98553	29.56	3336	31.07
Ryuk	Server-2019-Mid	93814	12.67	7289	68.4

Windows 10 High Specification

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-High	68.96	77.37	31.62	457.12	37.10	8	88500.41	28297.32	28647.71	15.05	168.35	23.63
Babuk	Win-10-High	38.54	94.80	93.48	376.90	37.86	8	3189.90	21838.42	21783.18	19.83	151.92	17.53
Blackmatter	Win-10-High	6.74	8.91	4.58	299.34	21.56	10	1598.82	8358.30	8351.87	10.45	108.34	15.39
Conti	Win-10-High	7.95	15.24	9.83	228.03	11.32	8	261.15	12402.19	12389.49	83.23	167.80	15.25
Darkside	Win-10-High	6.90	20.24	15.05	393.16	23.78	10	1665.17	8488.67	8470.35	10.75	114.21	17.02
Lockbit	Win-10-High	28.78	44.13	17.42	498.25	24.38	8	1440.13	1251.17	1417.23	9.20	119.75	20.38
Maze	Win-10-High	4.10	5.80	3.91	323.62	5.11	8	1564.34	10369.55	3806.94	3.70	85.59	14.08
Mespinoza	Win-10-High	6.23	7.29	4.68	144.07	2.24	8	147.27	7219.82	5397.70	3.58	61.30	8.30
Revil	Win-10-High	8.09	21.70	15.75	252.97	19.27	8	2732.09	17054.07	16986.81	10.48	100.22	14.25
Ryuk	Win-10-High	43.93	56.51	11.68	106061.45	64.46	8	1941.94	33521.11	41399.72	182.68	326.10	103.71

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-High	98560	14.10	6990.00	65.2
Babuk	Win-10-High	98560	6.52	15130.00	141
Blackmatter	Win-10-High	98553	45.23	2179	20.31
Conti	Win-10-High	98560	58.30	1691	15.76
Darkside	Win-10-High	98553	45.38	2172	20.24
Lockbit	Win-10-High	98548	5.40	18259	170
Maze	Win-10-High	98560	115.45	853.71	7.957
Mespinoza	Win-10-High	97080	115.60	839.83	7.828
Revil	Win-10-High	98553	23.70	4160	38.76
Ryuk	Win-10-High	98284	17.17	5740	53.37

Windows 10 Mid Specification

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-Mid	84.53	88.58	35.93	376.26	21.10	8	109298.88	31681.35	31810.25	8.82	145.11	18.33
Babuk	Win-10-Mid	28.88	92.38	91.30	342.77	21.67	8	2573.52	18024.88	17406.98	14.48	124.84	15.87
Blackmatter	Win-10-Mid	7.09	9.93	5.65	299.84	14.13	10	1713.94	9098.79	9079.02	9.82	98.72	14.88
Conti	Win-10-Mid	8.03	15.45	9.92	219.44	7.29	8	67.98	12578.51	12631.15	42.55	122.58	14.83
Darkside	Win-10-Mid	7.05	21.41	15.69	393.82	15.86	10	1647.89	8560.02	8550.47	10.30	104.35	16.85
Lockbit	Win-10-Mid	28.65	42.79	15.75	533.11	16.01	8	1319.68	1149.89	1246.13	10.74	111.46	20.72
Maze	Win-10-Mid	4.29	5.31	4.06	318.91	5.09	8	1561.72	10573.49	3707.72	3.63	82.95	13.79
Mespinoza	Win-10-Mid	6.39	7.56	4.79	144.08	2.23	8	137.56	7402.86	5527.32	3.58	61.26	8.23
Revil	Win-10-Mid	8.44	22.78	15.96	253.35	12.48	8	2710.56	16585.00	16521.51	9.70	91.44	14.05
Ryuk	Win-10-Mid	43.86	54.72	12.19	126006.82	63.22	8	1599.03	33496.12	41261.27	182.21	322.15	95.17

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-Mid	98560	12.63	7804.00	72.7
Babuk	Win-10-Mid	98560	7.84	12580.50	117
Blackmatter	Win-10-Mid	98553	42.92	2297	21.40
Conti	Win-10-Mid	98560	59.34	1661	15.48
Darkside	Win-10-Mid	98553	44.72	2204	20.54
Lockbit	Win-10-Mid	98548	5.84	16881	157
Maze	Win-10-Mid	98560	115.12	856.19	7.980
Mespinoza	Win-10-Mid	97080	114.20	850.09	7.924
Revil	Win-10-Mid	98553	23.67	4166	38.81
Ryuk	Win-10-Mid	87739	16.98	5270	48.15

About SURGe

Established in October 2021, SURGe is Splunk's strategic cybersecurity research arm dedicated to researching, responding and educating on the cyberthreats impacting the world. As a trusted advisor, SURGe provides organizations with technical guidance during high-profile, time-sensitive cyberattacks via response guides and in-depth analyses in research papers, conference papers, and webinars. Organizations can count on SURGe to provide appropriate context and timely recommendations to navigate global security incidents with confidence and intelligence. Learn more.

22-23023-Splunk-EmpiricallyComparativeAnalysisofRansomwareBinaries-WP-101