TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

The Technical Landscape of Ransomware: Threat Models and Defense Models

June 2023

Status: Ready for release

Distribution: Public

Barton P. Miller, Elisa R. Heymann, and Ishaan Kohli

About Trusted CI

The mission of Trusted CI is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program.

Acknowledgments

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grants #1920430 and #2241313. For more information about Trusted CI, please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Cite this work using the following information:

> Barton P. Miller, Elisa Heymann and Ishaan Kohli, “The Landscape of Ransomware”, June 2023. https://doi.org/10.5281/zenodo.8140464.

Contents

1 Introduction

Ransomware has become a global problem, striking almost every sector that uses computers, from industry to academia to government. These attacks affect the smallest businesses, the largest corporations, research labs, and have even shut down IT operations at entire universities[1,2].

While there have been many studies of the threats and risks associated with ransomware[3,4,5], in this document we take a more detailed technical approach. We start with a discussion of the basic attack goals of ransomware and distinguish ransomware from purely malicious vandalism. We present a canonical model of a computing system, representing the key components of the system such as user processes, the file system, and the firmware. We also include representative external components such as database servers, storage servers, and backup systems. This system model then forms the basis of our discussion on specific attacks.

We then use the system model to methodically discuss ways in which ransomware can (and sometimes cannot) attack each component of the system that we identified. For each attack scenario, we describe how the system might be subverted, the ransom act, the impact on operations, difficulty of accomplishing the attack, the cost to recover, the ease of detection of the attack, and frequency in which the attack is found in the wild (if at all). We also describe strategies that could be used to detect these attacks and recover from them.

Our goal is to present the broad landscape of how ransomware can affect a computer system and suggest how the system designer and operator might prepare to recover from such an attack. From this document, we will produce more concise versions that are focused prescriptions and best practices.

[1] "El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque" ("The Government allocates 3.5 million to the UAB to recover from the cyberattack"), *La Vanguardia,* November 23, 2021.
https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uab-recuperarse-ataque-informatico.html

[2] Scott Jaschik, "College Closes After 157 Years", https://www.insidehighered.com/news/2022/04/01/lincoln-college-illinois-close

[3] I. Nadir and T. Bakhshi, "Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques", *International Conference on Computing, Mathematics and Engineering Technologies (iCoMET),* Sukkur, Pakistan, March 2018.doi: 10.1109/ICOMET.2018.8346329.

[4] J. Hernandez-Castro J, A. Cartwright, E. Cartwright, "An economic analysis of ransomware and its welfare consequences", *Royal Society Open Science Journal* **7**, 190023, 2020. http://dx.doi.org/10.1098/rsos.190023

[5] "America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies", Committee on Homeland Security and Government Affairs, U.S. Senate, March 2022. https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

Note that in this document, we are focused on detection, recovery, and resilience. As such, we are explicitly not discussing how the ransomware might enter a computer system, nor are we discussing system vulnerabilities as there are extensive bodies of work on these topics. The topic of vulnerabilities that allow the attacker to enter the system is outside the scope of the document. The assumption is that the attacker did enter the system and rendered it inoperative to some extent using an attack based on human engineering, an unpatched known vulnerability, or even a zero-day vulnerability.

Takeaway 1: Your system **will** be successfully attacked so you must have a recovery and continuity of operations strategy.

Some of the ransomware scenarios that we describe reflect attacks that are common and well understood. Many of these scenarios have active attacks in the wild. Other scenarios are less common and do not appear to have any active attacks. In many ways, these less common scenarios are the most interesting ones as they pose an opportunity to build defenses ahead of attacks. Such areas need more research into the possible threats and defenses against these threats.

Based on our study, we present our major takeaway observations and best practices that can help make a system more resilient to attack and easier to recover after an attack.

Note that this document represents our best understanding of the current threats and attacks. As the technology and our understanding of the technology evolve, we will update this report. We actively solicit corrections, feedback, and contributions to make this document more accurate, complete, and timely. Please send your comments to the authors at `bart@cs.wisc.edu` and `elisa@cs.wisc.edu`.

2 Ransomware Attack Goals

Our focus in this document is on ransomware, that is software that causes payment to be extorted or else some penalty will be imposed. These penalties can come in two varieties:

1. The contents of the computer system are modified, typically encrypted or deleted, so that the system becomes inoperative. This modification is done in such a way that the attackers can restore the system to normal operations after a *ransom payment* is made.
2. Data from the computer system is exfiltrated. The attackers demand a *blackmail payment* to prevent the data from being revealed to the public.

Attacks can combine the above two varieties.

More precisely, we identify four basic operations that malware will conduct.

(ENC) *Encryption* is the most common operation taken by ransomware. This operation encrypts some portion of the storage of the victim system, promising to reverse the encryption if payment is made.

(LOC) *Lockout* prevents the user of the victim system from accessing all or part of the system functionality. A lockout might involve an operation such as changing a password, creating a password where none previously existed (such as for booting), or modifying critical code such as the BIOS or firmware.

(EXF) *Exfiltrating* data provides the attacker with potentially private, proprietary, or sensitive data taken from the victim system. The attacker then blackmails the system owner by threatening to reveal the private information.

(DEL) Deleting data prevents some or all of the normal system operation. For this to be ransomware, and therefore reversible, it must be combined with exfiltration.

We noted that (ENC), (LOC), and (DEL) are attacks on *availability* and (EXF) is an attack on *confidentiality*.

So, sensible combinations that could generate a ransom or blackmail payment are:

(ENC)	Ransom
(ENC) + (EXF)	Ransom and blackmail
(EXF)	Blackmail
(EXF) + (DEL)	Ransom and blackmail
(LOC)	Ransom
(LOC) + (ENC)	Ransom

We distinguish between a ransom attack and plain vandalism. Vandalism is an attack for which there is no meaningful payment option. These malware operations would be considered vandalism:

(DEL)
(ENC) with no ability to decrypt

Note that some of the categories that we mention are broadly understood and well discussed in the literature. For example, Rubrik[6] mentions both (ENC) and (LOC), though

[6] D. Norman, J. Knott and J. Hemming, "Lessons Learned: Recovering from Ransomware", April 2020. https://rubrik.com/resources/white-papers/20/recovering-from-ransomware

conflates the system model with the type of attack action. Zimba *et al*[7] mention (ENC) and (LOC), as well as scareware. Genç *et al*[8] also mentioned these two categories.

While there are some relevant similarities, in this paper we are not discussing vandalism.

> From the Oxford English Dictionary:
>
> *van · dal · ism:* action involving deliberate destruction of or damage to public or private property.
>
> *ran · som:* a sum of money or other payment demanded or paid for the release of a prisoner.
>
> *black · mail:* the action of demanding payment or another benefit from someone in return for not revealing compromising or damaging information about them.

For example, the NotPetya attack in 2018[9] on the Maersk shipping company wiped out the contents of the disks on the tens of thousands of computers on the Maersk worldwide corporate network. At first glance appeared to be ransomware, but it offered no functional payment option. NotPetya turned out to be malicious vandalism on a global scale.

Another important category of attack is the *apparent attack*[10], also known as *scareware*. Such an attack does not really encrypt data, exfiltrate data, or lock the system (beyond the skill of an experienced user). This category includes (1) fake virus alerts that convince the user to download and run a bogus virus scanner, (2) fake claims of exfiltrating compromising images or videos leading to a payment, and (3) weak screen locks that demand a payment to unlock. In each case, the attacker has not created an insurmountable obstacle, but convinces the inexperienced user that such a situation exists. These attacks are easy to launch and typically require little skill on the part of the user.

3 A Canonical System Model

We start with a simple model of the computer system that is being attacked, illustrated in Figure 1. The goal of this model is to represent the components of a system that might be attacked and the interactions between components that are also candidates for attack. Note

[7] A. Zimba, Z. Wang and L. Simukonda, “Towards Data Resilience: The Analytical Case of Crypto Ransomware Data Recovery Techniques”, *International Journal of Information Technology and Computer Science*, vol 10, no. 1, Jan 2018. DOI https://doi.org/10.5815/ijitcs.2018.01.05.

[8] Z. Genç, G. Lenzini and P. Ryan,”The cipher, the random and the ransom: A survey on current and future ransomware”, *Advances in Cybersecurity*, Ljubljana, Slovenia, 2017, https://orbilu.uni.lu/handle/10993/32574

[9] “NotPetya Technical Analysis”, LogRhythm Labs, July 2017. https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical-analysis-logrhythm-labs-threat-intelligence-report.pdf

[10] Thanks to Kevin Roundy of Norton Lifelock for suggesting mention of this category.

that we consider the system model to be a work in progress. As attacks evolve and as we learn more about the threat space, this model will evolve.

The enclosing “Host” gray box represents a single computer system that is under attack. All components that are outside that box reside on different computer systems, possibly in the same facility or possibly remote.

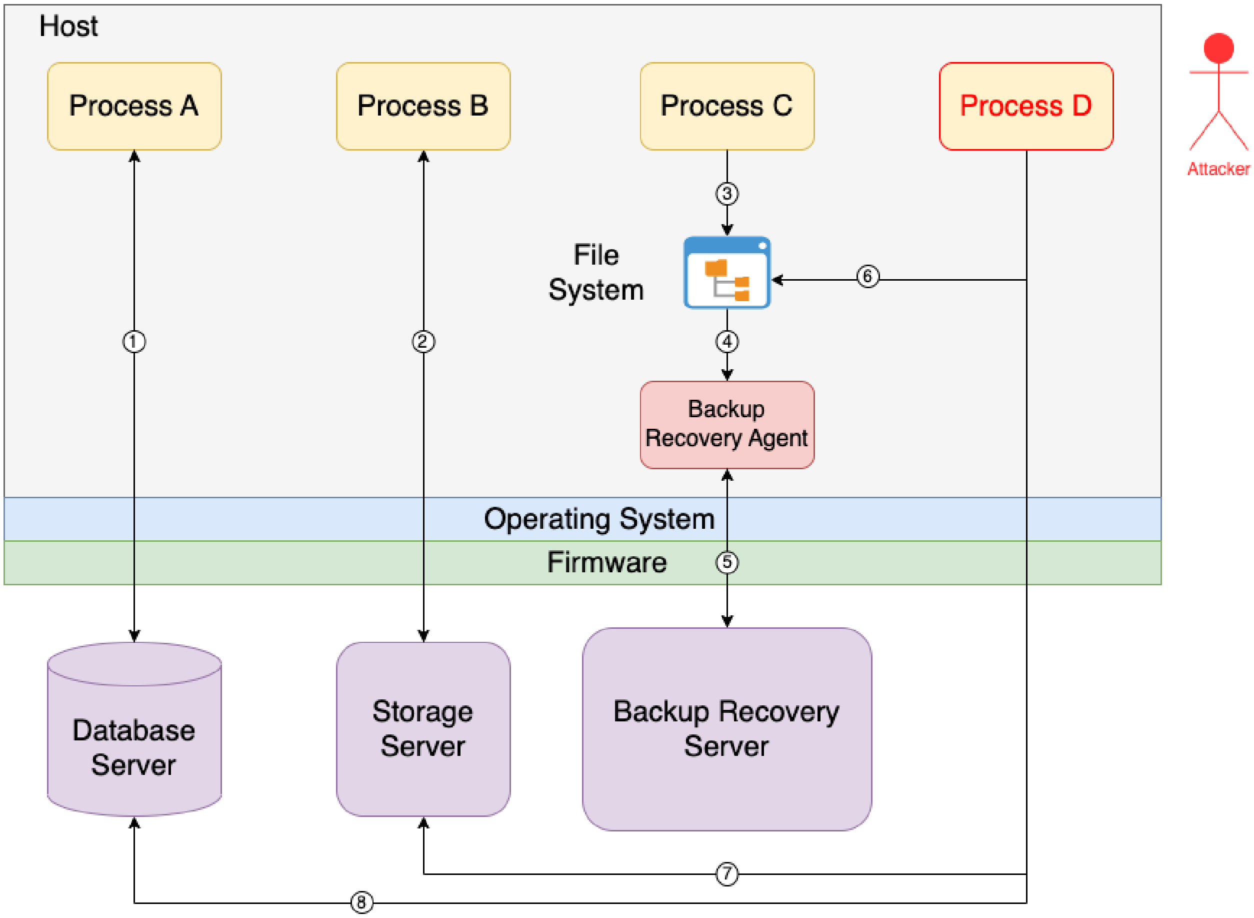

Figure 1: Canonical System

We start with three user processes, each of which is present to represent a different kind of ransomware attack.

Process A:	User program accessing an external database service that might be in the local facility or remote.
Process B:	User program accessing an external storage server (for example, a file server or storage appliance) that might be in the local facility or remote.

Process C: User program accessing the local file system.

Process D: An attacking program that will modify the system or contents of a remote server.

File System: Files that are stored on devices local to this host.

Backup Recovery Agent: Local service responsible for selecting files to be backed up and recovered.

Backup Recovery Server: External service supporting the backup and recovery of files. It might be local or remote.

Database Server: External service running in the local facility or remotely, accepting queries from Process A.

Storage Server: External service running in the local facility or remotely, accepting file system requests from Process B.

Firmware: Semi-permanent software embedded in the devices associated with the host. These devices might include the motherboard (BIOS/UEFI and boot code), hard drives, and network card.

We illustrate both the components of the system and interaction of the components because an attack can operate on data while it is stored, *data at rest* (RES), or data while it is being operated on or transferred, *data in motion* (MOT).

We also distinguish between attacks that affect the system (SYS), which includes the operating system kernel (including file system) and firmware, and those that affect user data and code (USR), which includes file system data and any process running on the local host (in our diagram, Processes A, B, and C, and the Backup Recovery Agent).

4 Attack Assumptions

As we have discussed, this document is focused on the recovery and resilience aspects of ransomware. As such, we are not discussing how the attacker can enter the system. We assume that there has been a successful exploit and the attacker has some level of control over the system. It is at that point, we are interested in how the attacker effects the ransom. What the attacker does at this moment determines how we should recover the system so that we can return to normal operation.

4.1 Attack Operations

Some of the basic operations that ransomware might use appear below. This list will evolve as our understanding of the threat space evolves.

(RWFILE) *Read, write, or create arbitrary files:* These files might be on a local file system or on a remote server. The access could result in an exfiltration, encryption, or deletion of files. It could also result in modification of system configuration information such as a password file.

(EXCODE) *Execute arbitrary code:* Executing any program on the system allows a wide range of control of the system. If you combine this operation with the ability to create or modify files, this means that any desired program or script can be created and executed. Included in this functionality is the ability to execute any system library function or kernel call and invoke an operation on any remote server.

(RPROC) *Inspect the state of any process (running program):* Any information contained in the execution state of a process is available for viewing. The debug interface or the UNIX `/proc` file system are common ways to access the state of a process. This access can be simplified by the use of packages like the Dyninst binary analysis and instrumentation toolkit[11] or the Red Hat SystemTap utility[12].

(WPROC) *Modify the state of any process:* In the same way that a process' state can be read, it can also be modified, including both the data and code using the same tools as mentioned above. So, any existing running program can have its behavior changed in an arbitrary way.

(WSYS) *Modify the state of the operating system:* A privileged attacker can modify the code or data within the operating system. This kind of attack can make arbitrary changes to the behavior of the operating system.

These operations are limited by the ability of the host to perform these operations. For example, the network might restrict which other hosts can be contacted and the types of protocols to reach them. Combining operations such as (EXCODE) and (RPROC) mean that any credential, such as an access token or certificate, held by a process can be subverted by

[11] "The DyninstAPI Binary Instrumentation and Analysis Toolkit", https://github.com/dyninst/dyninst/

[12] William Cohen, Don Domingo, Vladimír Slávik, Robert Kratky and Jacquelynn East, "SystemTap Beginners Guide", https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/systemtap_beginners_guide/index

an attacker. Combining (EXCODE) with (RWFILE) means that any access token or certificate stored in a file can be similarly subverted.

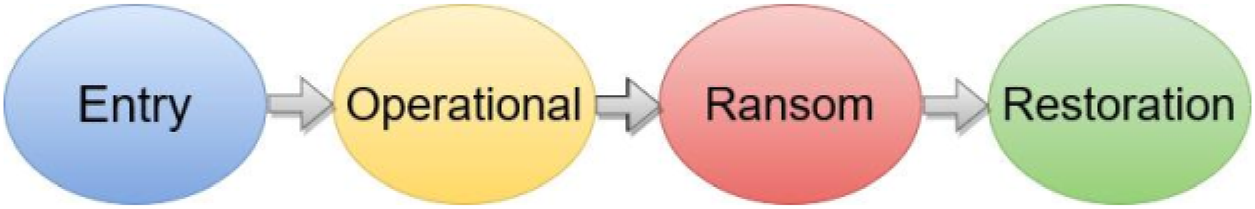

Figure 2: Workflow for a Successful Ransomware Attack

4.2 Attack Workflow

A ransomware attack goes through four basic stages, as shown in Figure 2.

The **entry stage** is based on the initial system exploit. This exploit might be based on a human engineering attack, a known vulnerability in software that has not been updated, or a previously undisclosed (zero day) attack. The human engineering attacks appear to be the most common, followed by attacks on systems that have not been updated. Undisclosed attacks most commonly come from well-funded organizations or nation-state operations. This part of the workflow is out of the scope of our discussion. This stage needs to be stealthy and may happen well in advance of the operational stage.

The **operational stage** is when the major damage to the system occurs. It is in this stage that data is encrypted, overwritten, deleted, or exfiltrated (or some combination of these). Depending on the type of attack, the damage might be immediately visible or only apparent later.

An attack that encrypts or removes stored data, i.e., data at rest, will immediately transition to the ransom stage, leaving the system non-functional. For this type of attack to be most effective, it should operate quickly to avoid detection and interruption.

An attack that encrypts the data in motion can allow the system to keep operating even though the data is encrypted. The system would be modified so that data is encrypted when written and decrypted when read. The attacker chooses the time of transition to the ransom stage by deleting the decryption key and shutting down the system.

Lockout attacks prevent future operation of the system by changing a password, creating a new one, or overwriting critical code. Once the modification has been made, the system typically continues to operate normally until the user logs out or the system restarts. The attacker can force the transition to the ransom stage by causing the logout or restart.

There are, however, types of attacks that will not disable the system at all. For example, a pure exfiltrate attack, whose main goal is blackmail to prevent the public release of the data, will not prevent continued system operations.

The **ransom stage requires** some form of payment to restore operation or prevent the release of private information. The victim trusts the attacker to cooperate once payment is made. However, it is in the best interest of the attacker to fulfill their side of the bargain or else they endanger payments from future victims.

For systems that were disabled, the **restoration stage** allows continuation of normal operations. If data was encrypted at rest or in motion, the attacker will provide a decryption key. If the data was deleted, the attacker will provide a restore program to download the files. If a password was modified or created, the attacker will provide this new password. If a system component (such as the BIOS) was modified, then the attacker will provide a key to tell the modified component to return to normal operations.

Of course, any payment of the ransom does not guarantee that there will be no future demands for payment. Only independent recovery will take the attacker out of the loop. Of course, the source of the initial exploit must also be determined and neutralized.

4.3 Detection and Recovery

As mentioned previously, we are not discussing techniques to prevent ransomware attacks as there is little difference in preventing ransomware attacks from preventing many other kinds of attacks. However, preventing and recovering from a ransomware attack has some unique properties.

Detection is often based on detecting changes in the system that are characteristic of a ransomware attack, such as the appearance of a significantly new area of encrypted data or of unusual changes to file metadata, such as encrypted file names or modified file access permissions.

Recovery is best characterized as having complete backups of affected system and its file data. We advocate a virtualization approach, where all critical systems are contained in virtual machine images (or possibly system containers) and stored in write-once archives. A large part of recovery then becomes restarting the affected system image on a physical or virtual (cloud) host. This approach is a best practice:

1. Create virtual machine (or system container) images for all critical systems and have recent versions archived (backed up) in a write-once storage system.

More details on detection and recovery are included in the threat discussions in the next section.

Scenario	Variation	Impact	Difficulty to Effect	Cost to Recover	Difficulty to Detect	Frequency in the Wild
FSA	(USR)(RES)(ENC)	Med-Hi	Med	Med	Med-Hi	24
	(USR)(RES)(EXF)(DEL)	Med-Hi	Med	Med	Low	0
	(USR)(RES)(EXF)(ENC)	Med	Med	Med	Low	30
	(USR)(SYS)(MOT)(ENC)	Hi	Hi	Hi	Med	0
	(USR)(LOC)	Med	Low	Med-Hi	Low-Med	10
SSA	(USR)(RES)(ENC)	Med-Hi	Med	Med	Med-Hi	15
	(USR)(RES)(EXF)(DEL)	Med-Hi	Med	Med	Low	0
	(USR)(RES)(EXF)(ENC)	Med	Med	Med	Low	20
	(USR)(SYS)(MOT)(ENC)	Hi	Hi	Hi	Med	0
	(USR)(LOC)	Med	Low	Med-Hi	Low-Med	0
DSA	(USR)(RES)(ENC)	Med-Hi	Med	Med	Med-Hi	0
	(USR)(RES)(EXF)(DEL)	Med-Hi	Med	Med	Low	0
	(USR)(RES)(EXF)(ENC)	Med	Med	Med	Low	0
	(USR)(SYS)(MOT)(ENC)	Low	Hi	Hi	Med	0
	(USR)(LOC)	Med	Low	Med-Hi	Low-Med	0
BSA	(SYS)(MOT)(ENC)(DEL)	Hi	Hi	Hi	Low	0
OSA	(SYS)(RES)(LOC)[13]	Hi	Hi	Hi	Hi	5
	(SYS)(RES)(LOC)[14]	Med	Med	Med	Low	3
FWA	(SYS)(RES)(LOC)	Hi	Hi	Hi	Hi	0

Table 1: Ransomware Scenarios and Attack Metrics

[13] Modifying the boot loader or boot block.

[14] Changing user passwords.

5 The Ransomware Threat Space

Given our canonical system model and our attack assumptions, we create a collection of threat scenarios, examining our system model one component at a time to understand how ransomware attempts to prevent recovery.

For these threats, we assume that there has been a successful exploit that has allowed the attacker to have full system ("root" or "administrator") access.

For each scenario, we discuss how the ransomware might subvert that component and how difficult it would be to recover after a successful attack to that component. We also evaluate how difficult it is to carry out the attack and how difficult it is to detect it.

For each scenario that has known attacks, we list the ones with which we are aware. Note that these scenarios are quite different from the NIST 1800-25[15] Data Integrity Test Cases, which are focused on protecting against malware entry rather than the ransom actions of malware. Some of the scenarios do not yet have known attacks, so these scenarios are of particular interest. The complete list of attacks that we know of appears in Section 7 with more detail presented in Appendix A.

5.1 File System Attacks (FSA)

Files are the most common target of a ransomware attack, whether it is for encryption, deletion, exfiltration, or lockout. A file system attack can come in many forms, some of which are common in the wild and some of which have not yet appeared. The FSA scenario can come in three forms, attacks on data at rest, data in motion, and file metadata.

5.1.1 FSA on Data at Rest

The Attack

The most common form of this attack is simple: read in a file (RFILE), encrypt the contents, and write it back out (WFILE). Such an attack might be caused by Process D via edge 6 in Figure 1. The most effective algorithms for this encryption are asymmetric (public key)

[15] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, and J. Sweetham, "Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events", *NIST Special Publication 1800-25, December 2020.*

algorithms[16,17] so that discovery of the encryption key will not allow the owner of the system to have any advantage in decrypting the data. However, encrypting a large amount of data with a public key algorithm can be a slow process. Such slowness increases the opportunity for the system owner to discover the attack before it completes, perhaps stopping it before all the data was encrypted. To counter that issue, ransomware FSA's will often use symmetric key algorithms (increasing the chance of key discovery) and encrypt only part of each file, say only the first megabyte[18,19,20,21].

An alternative to the encryption FSA is to exfiltrate a copy of data with the intent on releasing the data publicly (or in some other harmful sphere) if no payment is made. This type of an attack is more blackmail than ransom.Note that exfiltration increases the possibility of detection by a network-based intrusion detection system.

Of course, exfiltration and deletion can be combined to provide the threat of both ransom to restore the system and then ongoing blackmail to prevent public release of the data. Examples of this combination appear in Astrolocker [a][b], Babuk [e], Dark Slde [w][x][y], Maze [xx], and Ryuk [qqq][rrr].

Detection and Recovery

A recovery strategy from this type of FSA starts by making regular file system backups to a remote and safe server. Backing up files is a well understood and widely recommended

[16] Subedi, K., Budhathoki, D., & Dasgupta, D., "Forensic analysis of ransomware families using static and dynamic analysis", *IEEE Security and Privacy Workshops (SPW),* San Francisco, May 2018.

[17] O'Kane, P., Sezer, S., & Carlin, D. "Evolution of ransomware", Institution of Engineering and Technology Networks, vol. 7, no. 5, pp 321-327, Sep 2018, DOI https://doi.org/10.1049/iet-net.2017.0207.

[18] Palisse, H., Lanet, J.L., Le Guernic, C., & Legay, A. "Ransomware and the Legacy Crypto API", *Risks and Security of Internet and Systems,* Roscoff, France, vol 11, March 2017. DOI https://doi.org/10.1007/978-3-319-54876-0_2

[19] Genç, Z., Lenzini, G., & Ryan, P., "Next Generation Cryptographic Ransomware", *Secure IT Systems,* Oslo, Norway, vol 23, November 2018. DOI: https://doi.org/10.1007/978-3-030-03638-6_24

[20] T. McIntosh, J. Jang-Jaccard, P. Watters, and T. Susnjak,https://doi.org/10.1007/978-3-030-03638-6_24 "The Inadequacy of Entropy-Based Ransomware Detection", *Neural Information Processing,* Sydney, Australia, Dec 2019. DOI: 10.1007/978-3-030-36802-9_20.

[21] J. Han, Z. Lin, and D. E. Porter, "On the Effectiveness of Behavior-Based Ransomware Detection", *Security and Privacy in Communication Networks,* Washington, DC, vol 16, no. 3, Oct 2020. DOI: https://doi.org/10.1007/978-3-030-63095-9_7

practice to allow recovery from this type of attack[22,23,24,25]. Cloud providers such as Microsoft's Azure[26], Google Cloud[27], and Amazon AWS[28] have built-in facilities to help support such backups.

To ease the task of recovery and reduce the chance that this server will also be attacked, several **best practices** for backups should be followed:

[22] R. Richardson and M.M. North, "Ransomware: Evolution, Mitigation and Prevention", *International Management Review,* vol 13, no. 1,January 2017, https://digitalcommons.kennesaw.edu/facpubs/4276.

[23] L.Y. Connolly and D.S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures", *Computers & Security,* vol. 87, November 2019. DOI: https://doi.org/10.1016/j.cose.2019.101568

[24] F. Malecki, "Best practices for preventing and recovering from a ransomware attack," *Computer Fraud & Security,* vol. 2019, no. 3, January 2019. DOI: 10.1016/S1361-3723(19)30028-4.

[25] "S. Mohurle and M. Patil, "A Brief Study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5, May 2017.

[26] "Recover files from Azure virtual machine backup", March 2023. https://learn.microsoft.com/en-us/azure/backup/backup-azure-restore-files-from-vm

[27] "Back up data for disaster recovery", https://cloud.google.com/filestore/docs/backup-restore

[28] "Getting started 6: Restore a backup", https://docs.aws.amazon.com/aws-backup/latest/devguide/restore-resource.html

1. Backups should be "write once" or WORM, which means once they have been created, the server will not allow them to be modified. This is the "secure storage" criteria from NIST 1800-25.
2. The backup server should be physically secure.
3. Authentication and access to the server should be separate from other hosts. There should be a limited number of people that have access to the system and there should be a separate access enforcement mechanism. For example, the backup server should not be in the same Windows Active Directory Domain as other hosts.
4. File recovery should be tested on a regular basis.
5. Separate authorizations and permissions for each backup client's files.
6. Use monitoring tools such as Tripwire Enterprise[29], Netwrx Change Tracker[30], SolarWinds Security Event Manager[31], and Semperis Directory Services Protector[32] (for Active Directory) to detect when parts of the file system appear to have suspiciously encrypted content. Tripwire and Semperis are recommended in NIST SP 1800-25.
7. Limit the rate of backups that a client can make to prevent denial of service attacks that would push out relevant backups, fill storage quotas, or obscure the version history.

Cloud and storage products such as Polaris Radar[33] and Cloud environments such as Microsoft Azure[34] support such practices.

Once the attacked host has been cleared of the attack, then the file system data can be restored using normal file restoration procedures.

Takeaway 2: Have a well planned and practiced file recovery plan.

[29] "Enterprise: Detect Changes Before They Become Breaches", https://www.tripwire.com/products/tripwire-enterpriseTripwire https://www.netwrix.com/how_to_audit_file_permission_changes.html https://www.netwrix.com/file_integrity_monitoring_software.html

[30] "Netwrix Change Tracker", https://try.netwrix.com/tripwire_alternative_search_nnt

[31] https://www.solarwinds.com/security-event-manager/use-cases/file-integrity-monitoring-software

[32] "Directory Services Protector", https://www.semperis.com/ds-protector/

[33] Rubrik, "Defense in Depth with Polaris Radar", https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf

[34] "Store business-critical blob data with immutable storage", https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

5.1.2 FSA on Data in Motion

The Attack

Data in motion attacks will encrypt, delete, or exfiltrate data *as it is being written* to the file system, as shown by edges 3 and 4 in Figure 1. This type of attack would typically require the file system code in the operating system to be modified (WSYS), which makes this attack significantly more difficult to implement, likely explaining why such attacks have not yet been observed. Of course, we have no definitive way to know that such attacks do not exist or will not exist in the future. However, such an attack could result in a situation *where recovery, even with best practices in backup, would be extremely difficult.*

The basic idea for this attack is that the file system is modified so that all data that is written is encrypted before it is stored. When data is read back, it is decrypted so that the attack is not visible until the moment of the attackers choosing. In the background, the existing stored data (the data at rest) is encrypted with the same key. Note that this is a *stealthy attack* with no externally visible symptoms since a process that reads a file will see the correct data because the attack modification will decrypt the data on read.

The attack could be scheduled to be triggered at a certain time or based on a certain event or on demand by the attacker. Triggering the attack would cause the encryption/decryption key to be deleted from the computer's local memory. At this point, all file reads would return nonsensical (i.e., encrypted) data.

Note that since the system keeps operating while the files are encrypted, the backed up files will also be encrypted. This attack becomes more effective if the system is left to run for a longer period of time because the longer that the attack persists, the greater the change in the file system since the last unencrypted backup.

This attack might be discovered by tools that detect the presence of a large presence of anomalous or encrypted data in the file system. Such detection might also allow for the discovery of the encryption key, providing another aid in recovery.

Detection and Recovery

Recovery from this type of attack is problematic. If the attack was to persist for an extended period of time then the backup best practices described in Section 5.1.1 would not be effective. Such an attack will likely result in potentially significant data loss.

Early detection by use of file system monitoring tools can help limit the extent of such an attack (as mentioned in best practices from Section 5.1.1).

5.1.3 FSA on File System Metadata

The Attack

A file system attack is not limited to modifying the data stored in a file; it could also modify the information that describes how the data is stored, often called the *file metadata* (RWFILE). Examples of metadata that could be modified as part of an effective attack include the file names and access permissions. The most effective file name attack would be encryption of the file names. This attack is illustrated by Process D in Figure 1. Such attacks have included Lock [vv], Cryptowall [v], PC Cyborg [iii], and FuxSocy ENcryptor [gg], which modify the file names. In addition, there are attacks that encrypt other file system structural information, including Golden Eye [hh][ii] and Petya [hhh].

While the file contents (the data) would remain intact and accessible, such an attack would make finding the files problematic. At best, it would take an extended period of time to recover.

Detection and Recovery

A first line of defense is to detect if the file system metadata is ongoing any unusual modifications. Tools such as Netwrix and Tripwire (see Section 5.1.1) are designed to help with such tasks.

For effective recovery, a tool might be constructed that would compare the shape of the file system tree and file contents of the attacked file system to its most recent backup. Such a tool should be able to recover most of the file names. Note that ideally you do not want to simply restore a file system as that would lose any recent changes to the file contents. Though restoring to a recent backup would be better than losing complete access to the file system.

5.2 Storage Server Attacks (SSA)

In many ways, storage server attacks are similar to the FSAs: We are assuming that a privileged process can have arbitrary access to the files on the server in the same way as it would have access to local files (RWFILE), illustrated by Process D via edge 7 in Figure 1. As such, most of the discussions from Section 5.1, including the best practices, apply to SSAs. We note that many of the FSAs are also SSAs.

One way that this assumption is not true is that in an SSA, the server process is running on a different host, so it cannot modify the system software on that host (no WSYS). This limitation means that a comprehensive data-in-motion attack is not possible. While the attacker could intercept the reads and writes from the exploited host, it would not be able to intercept requests from other hosts. Under the data-in-motion attack, after data is written to a file in encrypted form but before the ransom act, file reads need to transparently decrypt the data.

In addition, depending on how the storage server is configured, the attacked host may not be able to access all the files (limited RWFILE) on the server nor have administrator access to that server.

A best practice is:

1. Having administrator access on a user's computer should not confer administrator access on another user's computer or on a server.

5.3 Database Server Attacks (DSA)

There are many similarities between a client process accessing a database server and a client process accessing a storage server, with the main difference being the access protocol. In the storage server case, access typically follows the basic open/read/write/close semantics of a file system. In the database server case, access follows a more structured protocol such as SQL.

With a DSA, we can still have attacks that encrypt the contents of the database (RWFILE), exfiltrate the data, or remove it, illustrated by Process D via edge 8 in Figure 1. We can also attack the database metadata by renaming relations or attributes and changing access permissions. In addition, we can intercept requests made by the client to the database server (WPROC), so can effect a data-in-motion attack. However, as with the SSA, we can only control the behavior of the clients on the attacked host and not those running on other hosts. This limits the effectiveness of such an attack.

Detection and Recovery

A recovery strategy from a DSA is similar to that used for a file system or storage server attack, a well designed and tested database backup and recovery strategy. If the host on which the database resides already has an effective file system recovery strategy, that may also include the databases stored there.

5.4 Backup System Attacks (BSA)

Backup systems play a key role in supporting system availability in response to both normal system and device failure and to an attack. Given this key role, the backup system itself becomes an attractive target for attack.

From the canonical system diagram (Figure 1), we can see that backups can be written to locally mounted disks or to a remote backup server. The attack has the same effect, whether backups are stored locally or remotely. The point of attack is the software on the local computer that identifies the files to be backed up and then writes them to storage, the Back Recovery Agent.

The Attack

A backup system attack modifies the data that is being written to the backup storage device or service by modifying the behavior of the Backup Recovery Agent (WPROC). For this modification to be a ransom activity and not vandalism, it must be reversible. For it to be an effective ransom activity, it must be difficult to reverse without special knowledge.

This attack proceeds through the stages described in Section 4.2 (Figure 2). During the entry stage, the attack modifies the backup software to encrypt all data that is backed up.

During the operational stage, any backups that are produced will be encrypted in such a way that the user cannot use them. The longer the system runs, the more data will be stored in an encrypted, and therefore useless backup. The backup software would also be modified so that any recovery requests made during the operational stage will properly decrypt the data. This recovery behavior ensures that the attack continues to be stealthy until the ransom phase is triggered.

The ransom phase is triggered by deleting the primary copy of the files from the file system and deleting the decryption key from the host. At this point, the files are gone and the backups are encrypted.

Detection and Recovery

Preventing an BSA is based on limiting the damage that can occur. Such limiting requires that we can detect when backup data is unexpectedly encrypted. Such detection might be accomplished by using a file system monitoring tool as described in the best practices listed in Section 5.1.

Recovery from such an attack is problematic as the primary data is gone and the secondary data is encrypted. The longer that this attack is stealthily present in the computer, the larger the percentage of data that is likely to be encrypted.

5.5 Firmware Attacks (FWA)

Firmware is the software that is provided by a device manufacturer and runs inside a device to control that device. It is separate from the operating systems and applications that run on the computer and is stored in separate memory local to the device it controls. Examples of firmware include the BIOS/UEFI that provides the lowest level interface with the computer, and the software that controls disks (hard drives), network interfaces (NIC), keyboards, motherboard/management processor, USB controller, and even the computer's battery. Each of these devices has its own separate computer processor chip and the firmware runs on that processor. There can be more than a dozen such processors that control devices in a typical desktop, rack mounted, or laptop computer.

While firmware security is getting increased attention in recent years[35,36,37], more research is needed on threat models and defenses related to attacks on firmware.

5.5.1 FWA Modifying the Firmware

The Attack

There have been significant firmware attacks in recent years[38,39,40,41]. In a ransomware context, taking control of a device's firmware (WSYS) can have serious security consequences, such as:

- Taking control of the BIOS/UEFI or disk firmware, allowing an attacker to prevent booting the system.
- Taking control of the keyboard firmware, allowing an attacker to set a boot password that would also prevent booting.
- Taking control of the disk controller firmware, allowing an attacker to hide files, modify them, or surreptitiously redirect access to substitute files.
- Taking control of the NIC firmware, isolating a computer (especially a server) or allowing illegal remote access and control.

[35] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno and Nasir Ghan,, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", *IEEE Communications Surveys & Tutorials* **3**, April 2019. DOI: https://doi.org/10.1109/COMST.2019.2910750

[36] M. Midler, K. O'Meara and A. Parisi, "Current Ransomware Threats",Report DM20-0436, Soft Engineering Institute, Carnegie Mellon University, May 2020.

[37] "Unit 42 Ransomware Threat Report", Palo Alto Networks, 2022.

[38] "Sean Metcalf, "Thunderstrike: EFI bootkits for Apple MacBooks via Thunderbolt & Option ROMs", https://adsecurity.org/?p=854

[39] Sergiu Gatlan, "New UEFI bootkit used to backdoor Windows devices since 2012", https://www.bleepingcomputer.com/news/security/new-uefi-bootkit-used-to-backdoor-windows-devices-since-2012/

[40] Alex Scroxton, "MoonBounce firmware bootkit shows advances in malicious implants", https://www.computerweekly.com/news/252512229/MoonBounce-firmware-bootkit-shows-advances-in-malicious-implants

[41] Pavel Shoshin, "Malware delivery through UEFI bootkit with MosaicRegressor", https://usa.kaspersky.com/blog/mosaicregressor-uefi-malware/23419/

- Taking control of the battery firmware[42], causing shutdown of the computer at will.

The U.S. Departments of Commerce and Homeland Security produced a report in February 2022[43] citing concerns about the security of firmware and its update process. This report provides a good background and overview of this problem.

The good news is that modern systems provide significant defenses against such attacks. These systems use features such as Intel Boot Guard[44] or AMD Hardware Validated Boot (HVB)[45] combined with the UEFI Secure Boot facility[46] to ensure that the UEFI has not been tampered with and the proper code is selected to execute. Such features have been available since around 2010 in UEFI version 2.4. Any reliable computer vendor will adhere to these standards as they are required by recent versions of Windows, MacOS, and Linux. Most modern computers are shipped by the OEM with these features enabled, though it is possible in some cases to disable them. The framework for these security features is described in NIST SP 800-147[47].

Such features start with processor-based security mechanisms that provide cryptographically strong storage of keys. This encrypted information is stored in the trusted platform module (TPM)[48] built into or alongside a processor chip. Unless you can open the chip and defeat its anti-tampering mechanisms, the data stored in the TPM can be considered reliable and secure. Each step of the boot process is protected, including updates to the BIOS/UEFI, boot loader, device firmware, and even the jump (“reset vector”) address used by the processor on start-up. The encrypted keys and certificates, combined with signing of each software update delivered to the computer from the vendor, make it difficult to replace any system component.

[42] C. Miller, “Battery Firmware Hacking”, DEF CON 19, Las Vegas, August 2011.
C. Miller, “Battery Firmware Hacking”, Black Hat, Las Vegas, August 2011.

[43] “America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies”, Committee on Homeland Security and Government Affairs, U.S. Senate, March 2022. https://www.hsgac.senate.gov/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf

[44] “Intel Hardware Shield - Below-the-OS Security”, Intel White Paper, May 2021. https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/hardware-shield-overview-brief.html

[45] “AMD Secure Technology”. https://ebrary.net/24869/computer_science/secure_technology

[46] Unified Extensible Firmware Interface Forum, https://uefi.org/specifications

[47] David Cooper, William Polk, Andrew Regenscheid, Murugiah Souppaya, “BIOS Protection Guidelines”, National Institute of Standards and Technology, *Special Publication 800-147,* April 2011.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

[48] Trusted Computing Group, “Trusted Platform Module (TPM) Summary”, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

Detection and Recovery

While a successful firmware attack can be difficult to do, recovery from such an attack can be extremely labor intensive. Such a recovery can require reprogramming the EEPROM or FLASH memory on the motherboard or in the devices themselves.

While the labor to recover a few computers is manageable, the cost to recover a large number of computers, such as found in a data center or corporate network, can be prohibitive.

NIST developed a standard for protecting firmware, detecting tampering with firmware, and, more importantly, for recovering from such tampering. This standard is described in SP 800-193[49]. Unfortunately, this standard is not widely adopted (as was SP 800-147). Until there are universal mechanisms for rapid recovery from firmware tampering, the impact of such attacks will remain high.

Best practices for detection and recovery include:

1. Ensure that your operating system is updated to the most recent release. The newest versions of the major operating systems, (Windows, Linux, MacOS) require signed software and (mostly) signed firmware and up to date hardware that supports TPM-based security.
2. Ensure that Secure Boot has not been disabled. You can do this from the UEFI settings at boot time. Note that each vendor organizes their UEFI menus in a different way, so you may need to do a bit of searching or look at documentation from your computer vendor.
3. Ensure that the TPM has not been disabled. This can be done from the UEFI setting as for the previous item.
4. Use available tools, such as Eclypsium[50] or Binarly[51], to scan for unauthorized firmware changes.

Takeaway 3: Firmware is a rarely considered security issue. While there are tools to help detect malware attacks, there are many aspects that are not well understood and need more research.

[49] Andrew Regenscheid, "Platform Firmware Resiliency Guidelines", National Institute of Standards and Technology, *Special Publication 800-193,* May 2018. https://doi.org/10.6028/NIST.SP.800-193

[50] "Firmware Security for Enterprises", Eclypsium, https://eclypsium.com/enterprise-firmware-security/

[51] https://www.binarly.io/, free tool: https://www.fwhunt.run/

5.5.2 FWA Setting a Boot Password

The Attack

A standard security feature of modern computer systems is the ability to set a boot-time password. As its name implies, a password is required before the BIOS/UEFI will start the boot sequence. These passwords do not require any special permission to set, however this functionality on most computers requires that the password be typed on the keyboard. In a properly functioning system, it should not be possible to set this password under program control (even as root or administrator) or remotely as the BIOS/UEFI will enforce "proof of presence" at the keyboard to accept a password.

Subverting protections on setting a boot password could be done by subverting the keyboard firmware (WSYS). If the keyboard says that a person is present and entering a password, then the operating system is likely to believe it. However, as noted in the previous section, there are significant challenges to subverting device firmware. For systems that allow remote administration, such as servers with hardware to allow remote keyboard, monitor (video), and mouse access using a KVM switch[52], the ability to subvert the switch would allow the equivalent of physical presence at the systems' keyboards.

Detection and Recovery

The boot password is usually stored in separate volatile CMOS RAM on the motherboard. The battery on the motherboard that powers the RAM needs to be physically disconnected to reset any security data stored in this RAM. Such disconnection may involve unsoldering the battery connection, an activity that could require an overwhelming amount of work in a large enterprise.

A best practice for prevention is to

1. Have a boot password already set on your computer.

5.6 Operating System Attacks (OSA)

5.6.1 OSA on the Boot Loader and Boot Image

The Attack

The boot loader is the software responsible for initial loading of the operating system kernel. This loading is commonly done in two steps, where the BIOS/UEFI first loads a

[52] https://en.wikipedia.org/wiki/KVM_switch

simple program from a fixed location (often the first sector) on the boot device, and this program then finds and loads the full boot loader. The boot loader then goes on to load the operating system kernel. As described in Section 5.5, there is a cryptographically secured chain of steps that ensures that only software that originated from the vendor will be booted.

A successful attack on the boot loader or operating system boot image (WSYS) will prevent the operating system from starting. Until this situation is repaired, the computer will be unusable until it can be booted from an alternative device, such as a FLASH memory drive. This alternative booting might require an update to the BIOS/UEFI configuration as it is a common security practice to disable booting from alternative devices. Further, updating the configuration might be password protected, requiring the attention of a system administrator.

Detection and Recovery

The Secure Boot feature, along with Boot Guard or Hardware Validated Boot, will prevent an attacker from replacing the boot loader or operating system boot image. However, it will not prevent a vandalism attack that overwrites these items with non-functional code, such as was done for NotPetya attack on Maersk's shipping network.

Most operating systems (including Windows, MacOS, and Linux) offer the ability to boot from removable media (such as a USB memory stick) or the network. Once this is done, then the boot loader or operating system image can be restored. Such operation requires physical presence at the computer, so it is reasonable for recovering individual computers but expensive for large facilities or data centers.

Best practices for this situation are the same as those described for firmware attacks in Section 5.5**.**

5.6.2 OSA on Account Passwords

The Attack

A simple attack is to change the passwords for users and administrators (RWFILE). Such an attack will prevent normal access to the computer though it may not prevent services from starting on booting the system.

Detection and Recovery

As mentioned in the previous section, most operating systems (including Windows, MacOS, and Linux) offer the ability to boot from removable media (such as a USB memory stick) or the network. Once this is done, then the password file(s) can be restored. Such operation requires physical presence at the computer, so it is reasonable for recovering individual computers but expensive for large facilities or data centers. Note that if you boot from an alternate device and disk encryption, such as Microsoft BitLocker is enabled, then you will not be able to access the contents of the original disk unless you have the BitLocker key escrowed.

Best practices here include:

1. As for regular files: make sure that files that store login authentication data are included in the regular backups.
2. Ensure that you have escrowed the disk encryption keys for all the storage devices on all your systems.

6 Conclusion

Ransomware continues to be a serious threat affecting computer systems in every domain. Until we evolve away from computing paradigms where a simple miss-click can compromise an entire organization, this threat will not be reduced. In this document, we were making the assumption that the attacks will succeed, so we, as a community, need to focus on detection and recovery.

Our goal was to provide a broad picture of the way that ransomware could threaten a system. Where the threat is currently well understood and there are tools and best practices, we described them. Where threats are not so well understood (such as for firmware), we present the issues in the hope that researchers and enterprises will develop tools in these areas ahead of the attackers.

While we have presented a variety of of takeaways and best practices, there are a few messages that should be reiterated here:

1. All the normal defense measures that are advocated as best practices will help to reduce the incidence of ransomware. However, with current technology, a dedicated adversary will get in. The only recourse is to have effective detection and recovery mechanisms.
2. Use tools whenever possible for detecting ransomware attacks. While these tools do not cover the whole spectrum of attacks that we have presented, they do cover many of the most common current attacks.
3. Virtualize. By ensuring that every system that you run is enclosed in a virtual machine or container, you significantly simplify the restoration after a successful attack.

As we said in the introduction: This document represents our best understanding of the current threats and attacks. As the technology and our understanding of the technology evolve, we will update this report. We actively solicit corrections, feedback, and contributions to make this document more accurate, complete, and timely. Please send your comments to the authors at `bart@cs.wisc.edu` and `elisa@cs.wisc.edu`.

7 Reported Attacks

[a] “Sophos Links Mount Locker to **Astro** Locker Ransomware - Infosecurity Magazine”, https://www.infosecurity-magazine.com/news/sophos-mount-locker-astro-locker/

[b] “What is **Astro** Locker Team? - AlienVault - Open Threat Exchange”, https://otx.alienvault.com/pulse/606c9900cc9dabf9542b6d8d/, May 2021

[c] Yuste, J., & Pastrana, S. (2021). **Avaddon** ransomware: An in-depth analysis and decryption of infected systems. Computers & Security, 109, 102388. doi:10.1016/j.cose.2021.102388

[d] "Indicators of Compromise Associated with **AvosLocker** Ransomware", Federal Bureau of Investigation, US Treasury and The Department of Treasury, CU-000164-MW, March 2022

[e] "What Is **Babuk** Ransomware? | SiteLock", https://www.sitelock.com/blog/what-is-babuk-ransomware/, November 2021

[f] "**Bad Rabbit** Ransomware | KnowBe4", https://www.knowbe4.com/bad-rabbit-ransomware

[g] "**Bad Rabbit** ransomware | Securelist", https://securelist.com/bad-rabbit-ransomware/82851/, October 2017

[h] "What is **BadRabbit** Ransomware? Our Experts Explain All", https://airbus-cyber-security.com/badrabbit-ransomware/, November 2017

[i] "**BlackCat** Ransomware & Triple Extortion (Analysis & Tactics)", https://www.avertium.com/resources/threat-reports/blackcat-ransomware-triple-extortion-analysis-tactics, February 2022

[j] "Threat Assessment: **BlackCat** Ransomware", https://unit42.paloaltonetworks.com/blackcat-ransomware/, January 2022

[k] "Indicators of Compromise Associated with **BlackByte** Ransomware", US Secret Service, Federal Bureau of Investigation, CU-000163-MW, 11th February 2022

[l] "Modus operandi of **BlackByte** ransomware - Infosec Resources", https://resources.infosecinstitute.com/topic/modus-operandi-of-blackbyte-ransomware/, 23rd February 2022

[m] "**BlackByte** Ransomware – Pt. 1 In-depth Analysis | Trustwave", https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/, 15th October 2021

[n] "**BlackMatter** Ransomware", Cybersecurity and Infrastructure Security Agency, AA21-291A, 18th October 2021

[o] "**BlackMatter** Ransomware: In-Depth Analysis & Recommendations | Varonis", https://www.varonis.com/blog/blackmatter-ransomware, 2nd November 2021

[p] "Ransomware Spotlight: **Clop** - Security News", https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop, 22nd February 2022

[q] "**Clop** ransomware gang doxes two new victims days after police raids | TechCrunch", https://techcrunch.com/2021/06/23/clop-ransomware-gang-doxes-two-new-victims-days-after-police-raids/, 23rd June 2021

[r] "**Conti** Ransomware", Cybersecurity and Infrastructure Security Agency, AA21-265A, 22nd September 2021

[s] "TAU Threat Discovery: **Conti** Ransomware", VMware Security Blog - VMware, 8th July 2020

[t] "**CryptoLocker**: Everything You Need to Know", https://www.varonis.com/blog/cryptolocker, 29th March 2020

[u] Hansberry A, Lasse A, Tarrh A. "**Cryptolocker**: 2013's most malicious malware". Retrieved February. 2014;9:2017.

[v] "**CryptoWall** Ransomware. Everything you need to know", https://heimdalsecurity.com/blog/cryptowall-ransomware/, 8th February 2022

[w] "**DarkSide** Ransomware as a Service (RaaS)", US Department of State, 4th November 2021

[x] "What We Know About **Darkside** Ransomware and the US Pipeline Attack", https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html, 12th May 2021

[y] "**Darkside** Ransomware does not attack hospitals, schools and governments - Acronis", https://www.acronis.com/en-us/cyber-protection-center/posts/darkside-ransomware/, 29th November 2020

[z] "**Devil** Ransomware - Decryption, removal, and lost files recovery (updated)", https://www.pcrisk.com/removal-guides/16699-devil-ransomware, 8th August 2022

[aa] "**DMA Locker** Ransomware targets Unmapped Network Shares", https://www.bleepingcomputer.com/news/security/dma-locker-ransomware-targets-unmapped-network-shares/, 8th February 2016

[bb] "**DMA Locker** 4.0: Known ransomware preparing for a massive distribution | Malwarebytes Labs", https://www.malwarebytes.com/blog/news/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution, 23rd May 2016

[cc] "An Overview of the **DoppelPaymer** Ransomware", https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

[dd] "What is **Egregor** Ransomware? One of the Worst Threats of 2020 | UpGuard", https://www.upguard.com/blog/what-is-egregor-ransomware, 5th June 2022

[ee] "Mobile ransomware: major threats and best means of protection | Kaspersky official blog", https://usa.kaspersky.com/blog/mobile-ransomware-2016/7346/, 29th June 2016

[ff] "A look at the top seven ransomware attacks in the past decade - Help Net Security", https://www.helpnetsecurity.com/2017/11/28/top-seven-ransomware-attacks/, 28th November 2017

[gg] "New **FuxSocy** Ransomware Impersonates the Notorious Cerber", https://www.bleepingcomputer.com/news/security/new-fuxsocy-ransomware-impersonates-the-notorious-cerber/, 25th October 2019

[hh] "What is **GoldenEye** Ransomware & How to Protect Against It in 2022?", https://www.comparitech.com/net-admin/goldeneye-ransomware/, 17th July 2021

[ii] "Everything you need to know about the **Goldeneye**/Petya attack",https://www.bitdefender.com/blog/hotforsecurity/everything-you-need-to-know-about-the-goldeneye-petya-attack, 28th June 2017

[jj] "Tactics, Techniques, and Indicators of Compromise Associated with **Hello Kitty/FiveHands** Ransomware", Federal Bureau of Investigation - Cyber Division, CU-000154-MW, 28th October 2021

[kk] "**FiveHands** Ransomware", Cybersecurity and Infrastructure Security Agency, AR21-126A, 6th May 2021

[ll] "What Is the **HelloKitty** Ransomware? - Software Tested", https://softwaretested.com/anti-malware/what-is-the-hellokitty-ransomware/,

[mm]"**Hive** Ransomware", US Department of Health and Human Services, Health Sector Cybersecurity Coordination Center, Office of Information Security, 202110211300, 21st October 2021

[nn] "**HIVE** Ransomware: Everything You Need To Know (Attacks & Analysis)", https://www.avertium.com/resources/threat-reports/hive-ransomware-attacks-analysis, 16th November 2021

[oo] "Indicators of Compromise Associated with **Hive** Ransomware", Federal Bereau of Investigation - Cyber Division, MC-000150-MW, 25th August 2021

[pp] "**Jigsaw** Ransomware | KnowBe4", https://www.knowbe4.com/jigsaw-ransomware

[qq] Byrne D, Thorpe C. "**Jigsaw**: An investigation and countermeasure for ransomware attacks". In European Conference on Cyber Warfare and Security 2017 Jun 1 (pp. 656-665). Academic Conferences International Limited.

[rr] "Indicators of Compromise Associated with **LockBit** 2.0 Ransomware", Federal Bureau of Investigation - Cyber Division, CU-000162-MW, 4th February 2022

[ss] "**LockBit** ransomware — what is it and how to stay safe", https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

[tt] "What You Need to Know About the **LockerGoga** Ransomware - Security News", https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware, 20th March 2019

[uu] "What is **LockerGoga** ransomware? | Nomios Group", https://www.nomios.com/resources/what-is-lockergoga-ransomware/

[vv] "What is **Locky** Ransomware? Prevention information 2022", https://www.cybertalk.org/what-is-locky-ransomware/

[ww] "The **Locky** Ransomware Encrypts Local Files and Unmapped Network Shares", https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/, 16th February 2016

[xx] "What is **Maze** Ransomware and How Does it Work?", https://www.datto.com/blog/what-is-maze-ransomware-and-how-does-it-work?

[yy] "How **MedusaLocker** Ransomware Aggressively Targets Remote Hosts - SentinelOne", https://www.sentinelone.com/blog/how-medusalocker-ransomware-aggressively-targets-remote-hosts/, 28th November 2019

[zz] "**MegaCortex** Ransomware Information", https://success.trendmicro.com/dcx/s/solution/1122802-megacortex-ransomware-information?language=en_US, 30th December 2019

[aaa] "**MegaCortex**", New Jersey Cybersecurity and Communications Integration Cell, 8th May 2019

[bbb] "Petya is back and with a friend named **Mischa** Ransomware", https://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/, 12th May 2016

[ccc] "**Mount Locker** Ransomware Aggressively Changes Up Tactics | Threatpost", https://threatpost.com/mount-locker-ransomware-changes-tactics/165559/, 22nd April 2021

[ddd] "**Mount Locker** Ransomware Steps up Counter-IR Capabilities, Hindering Efforts for Detection, Response and Investigation | GuidePoint Security", https://www.guidepointsecurity.com/blog/mount-locker-ransomware-steps-up-counter-ir-capabilities/

[eee] "**Nemty** Ransomware Loves You", James Barnett, Inflobox, https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-nemty-ransomware-loves-you.pdf

[fff] "**Nemty** Ransomware - Learning by Doing | McAfee Blog", https://www.mcafee.com/blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/, 2nd April 2020

[ggg] "**NetWalk** Ransomware", Health Sector Cybersecurity Coordination Center, 202009241030, 24th September 2020

[hhh] "What is **Petya** Ransomware | Protect & Detect | Avast", https://www.avast.com/c-petya

[iii] "Case Study: AIDS Trojan Ransomware - SDxCentral, https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-aids-trojan-ransomware/, 3rd June 2020

[jjj] "**Phoenix** Cryptolocker Ransomware - NHS Digital", NHS Digital, CC-3813

[kkk]"Threat Analysis Report: Inside the Destructive **PYSA** Ransomware", https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-destructive-pysa-ransomware, 27th September 2021

[lll] "**Ragnar Locker** ransomware - what you need to know", https://www.tripwire.com/state-of-security/security-data-protection/ragnar-locker-ransomware-what-you-need-to-know/, 10th March 2022

[mmm] "**RagnarLocker** Ransomware Indicators of Compromise", Federal Bereau of Investigation - Cyber Division, CU-000163-MW, 7th March 2022

[nnn] "**RansomExx** - Who They Are & How to Protect Yourself From Them", https://www.titanhq.com/blog/ransomexx-who-they-are-and-how-to-protect-yourself-from-them/, 8th March 2021

[ooo] "Expanding Range and Improving Speed: A **RansomExx** Approach", https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html, 6th January 2021

[ppp]"What is **REvil** ransomware? | Nomios Group", https://www.nomios.com/resources/what-is-revil-ransomware/,

[qqq]"**RYUK** Ransomware", https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

[rrr] "**Ryuk** explained: Targeted, devastatingly effective ransomware | CSO Online", https://www.csoonline.com/article/3541810/ryuk-explained-targeted-devastatingly-effective-ransomware.html, 19th March 2021

[sss] "**SamSam** Ransomware", Cybersecurity and Infrastructure Security Agency, AA18-337A, 3rd December 2018

[ttt] "MAR-10166283.r1.v1 – **SamSam2**", Cybersecurity and Infrastructure Security Agency, AR18-337B, 3rd December 2018

[uuu] "**Snatch** ransomware reboots PCs into Safe Mode to bypass protection – Sophos News", https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/, 9th December 2019

[vvv] Taking a deep dive into **Sodinokibi** ransomware", https://www.acronis.com/en-us/cyber-protection-center/posts/sodinokibi-ransomware/, 3rd July 2019

[www] "**SynAck** ransomware group releases decryption keys as they rebrand to El_Cometa | ZDNET",

https://www.zdnet.com/article/synack-ransomware-group-releases-decryption-keys-as-they-rebrand-to-el-cometa/, 13th August 2021

[xxx] "**SynAck** Ransomware Leverages Process Doppelgänging for Evasion and Infection - Security News", https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/synack-ransomware-leverages-process-doppelg-nging-for-evasion-and-infection, 11th May 2018

[yyy] "**SynAck** targeted ransomware uses the Doppelgänging technique | Securelist", https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/, 7th May 2018

[zzz] "**Thanos** Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa", https://unit42.paloaltonetworks.com/thanos-ransomware/, 4th September 2020

[aaaa] "The current state of ransomware: **TorrentLocker** – Sophos News", https://news.sophos.com/en-us/2015/12/23/the-current-state-of-ransomware-torrentlocker/, 23rd December 2015

[bbbb] "**VICE SOCIETY** Ransomware - Decryption, removal, and lost files recovery (updated)", https://www.pcrisk.com/removal-guides/21962-vice-society-ransomware, 21st July 2022

[cccc]"What is **WannaCry** ransomware, how does it infect, and who was responsible? | CSO Online", https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html, 30th August 2018

Appendix A: Known Attacks

Ransomware	Time Range	(ENC) (LOC) (EXF) (DEL)	Attack Scenario	(MOT) vs. (RES)	(USR) vs. (SYS)	Cited
Astrolocker	2021 -	ELX	FSA, SSA	R	US	[a][b]
Avaddon	2020 - 2021	EX	FSA, SSA	R	U	[c]
Avoslocker	2021 -	E	FSA, SSA	R	U	[d]
Babuk	2021	EX	FSA	R	U	[e]
Bad Rabbit	2017	EL	FSA, SSA, OSA	R	US	[f][g][h]
Bitpaymer	2017 - 2018	ELX	FSA, SSA, OSA	R	US	Rebrand of DoppelPaymer
Black cat	2022 -	EX	FSA	R	U	[i][j]
Blackbyte	2021 -	E	FSA, SSA	R	U	[k][l][m]
Blackmatter	2021 -	E	FSA, SSA	R	U	[n][o]
Cerber	2016 - 2018	EX	FSA, SSA	R	U	Rebrand of REvil
Clop gang	2021	EX	FSA, SSA	R	U	[p][q]
Conti	2020 -	E	FSA, SSA	R	U	[r][s]
Cryptolocker	2013	E	FSA, SSA	R	U	[t][u]
Cryptowall	2014	EL	FSA	R	US	[v]
Dark side	2020	EX	FSA, SSA	R	U	[w][x][y]
Defray777	2017 - 2020	EX	FSA, SSA	R	U	Rebranding of Rasome

						xx
Devil	2019	E	FSA, SSA	R	U	[z]
DMA Locker	2016 - 2018	E	FSA, SSA	R	U	[aa][bb]
DoppelPaymer	2019 - 2020	ELX	FSA, SSA, OSA	R	US	[cc]
Egregor	2021 -	EX	FSA, SSA	R	U	[dd]
Fusob	2015 - 2016	E	FSA	R	U	[ee][ff]
FuxSocy Encryptor	2019 - 2020	EL	FSA	R	US	[gg]
Gandcrab	2018 - 2020	EX	FSA, SSA	R	U	Rebranding of REvil
Golden eye	2017	EL	FSA, OSA	R	US	[hh][ii]
Grief	2021 -	EX	FSA	R	U	Rebranding of DoppelPaymer
Hello kitty/Fivehands	2021 -	EX	FSA, SSA	R	U	[jj][kk][ll]
Hive	2021 -	EX	FSA	R	U	[mm][nn][oo]
Jigsaw	2016	ED	FSA, SSA	R	U	[pp][qq]
Lockbit	2021 -	EX	FSA, SSA	R	U	[rr][ss]
Lockergoga	2019 - 2021	EL	FSA, SSA, OSA	R	US	[tt][uu]
Locky	2016 - 2017	EL	FSA, SSA	R	US	[vv][ww]
Maze	2019 - 2020	EX	FSA	R	U	[xx]
Medusa Locker	2019 -	E	FSA, SSA	R	U	[yy]
MegaCortex	2019	EX	FSA	R	U	[zz][aaa]

Mischa	2016 - 2017	E	FSA	R	U	[bbb]
Mount locker	2020 - 2021	ELX	FSA, SSA	R	US	[ccc][ddd]
Nemty	2019 - 2020	E	FSA	R	U	[eee][fff]
Netwalker	2019 - 2020	ED	FSA, SSA	R	U	[ggg]
Payload.bin	2021 -	EX	FSA	R	U	Rebrand of Babuk
PC Cyborg	1989	L	FSA	R	S	[iii]
Petya	2016 - 2017	L	FSA, OSA	R	US	[hhh]
Phoenix locker	2021 -	E	FSA, SSA	R	U	[jjj]
Pysa	2019 -	EX	FSA, SSA	R	U	[kkk]
Ragner locker	2020 -	E	FSA, SSA	R	U	[lll][mmm]
RansomExx	2021 -	EX	FSA, SSA	R	U	[nnn][ooo]
REvil	2020 -	EX	FSA, SSA	R	U	[ppp]
Ryuk	2018 - 2020	EX	FSA, SSA	R	U	[qqq][rrr]
Samsam	2018 - 2020	E	FSA, SSA	R	U	[sss][ttt]
Sekhmet	2020	EX	FSA	R	U	Rebrand of Maze
Snatch	2019 -	EX	FSA	R	U	[uuu]
Sodinokibi	2020 -	EX	FSA, SSA	R	U	[vvv] (REvil)
SynAck	2018	EX	FSA, SSA	R	U	[www][xxx][yyy]
Thanos	2020 - 2021	ELX	FSA, OSA, SSA	R	US	[zzz]

Torrentlocker	2014 - 2016	E	FSA	R	U	[aaaa]
Vasa locker	2020 - 2021	EX	FSA	R	U	Rebrand of Babuk
Vice society	2021 -	EX	FSA	R	U	[bbbb]
Wannacry	2017	E	FSA	R	U	[cccc]