MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

REvil PAPER: SUMMARY AND OVERVIEW

Jaclyn Lasky, Chris Naughton, and Eric Arnoth

Abstract

This paper is a short summary and highlight of the main sections in the full REvil ransomware deep-dive paper. It covers mainly descriptions of Section 2, which details the techniques used by the REvil ransomware variant and its operators. This shorter paper will also cover highlights from Sections 3 and 4, but larger details can be found in the full document.

Table of Contents

List of Tables

Ransomware and REvil Overview

Section 1 of the full paper covers the introduction of ransomware in relation to the healthcare sector and provides background information on the REvil variant. This paper will cover a subset of sections from the full REvil document to make it easier to consume.

Ransomware Introduction

The incidence of ransomware attacks has increased during the past two years, for the healthcare sector and for other industries. The Health Sector Cybersecurity Coordination Center of the Department of Health and Human Services reports that as of May 25, 2021, they had tracked a total of 82 ransomware incidents globally during the calendar year that impacted institutions in the Health and Public Health sector. (Program, 2021) The effect of ransomware on victim organizations can be devastating, potentially crippling operations and making critical data unavailable. In the healthcare sector, the impact of ransomware has the potential to translate into lost lives of the patients in the care of an impacted institution.

Ransomware Impact on Healthcare Industry

The impact of ransomware on the healthcare industry is often more severe due to the nature of the work. Medical devices directly touch and interact with patients, being used not only for monitoring their health condition, but also to treat them. They are connected to humans on one end and connected to the network on the other end. The impact to these operational technology systems and an already overburdened information technology (IT) staff can be catastrophic, resulting in potentially lethal outcomes to the patients under the care of the targeted institution. Beyond the physical aspect, the safety and sensitivity of patient health information is also at risk. Securing both the physical health and privacy health of patients is necessary. Private health information often resides on such equipment, meaning a breach can result in data privacy issues,

REvil Characteristics and Background

Adversaries using REvil have demonstrated a determination to cause high impact. They often use a method called double extortion, in which they will demand an additional ransom to prevent the public release of stolen data. Beyond publicly shaming victims with the information stolen during their operation, the malware operators may also auction off stolen data.

REvil is also considered an affiliate model ransomware-as-a-service (RaaS). This means that it is not for sale in the traditional manner of commodity malware. REvil operators work with skilled affiliates, meaning the ransomware operators gain access through initial access brokers that get a share of the profits. Part of the reason REvil has been so damaging is that it relies on this affiliate model, meaning the operators specifically require technical sophistication to deploy it. It shares code similarities with GandCrab RaaS, which operated as a traditional RaaS for sale on the dark web, and there are claims that REvil is a continuation of the GandCrab ransomware. (Intel471, 2020)

When looking at ransomware examples, if one of them does not list any or many adversary groups using it, then consider looking at other ransomware software and examine those threat actors. This will help give broader insight into groups using ransomware, especially if that ransomware is used against the same industry.

REvil's Attacks on the Healthcare Industry

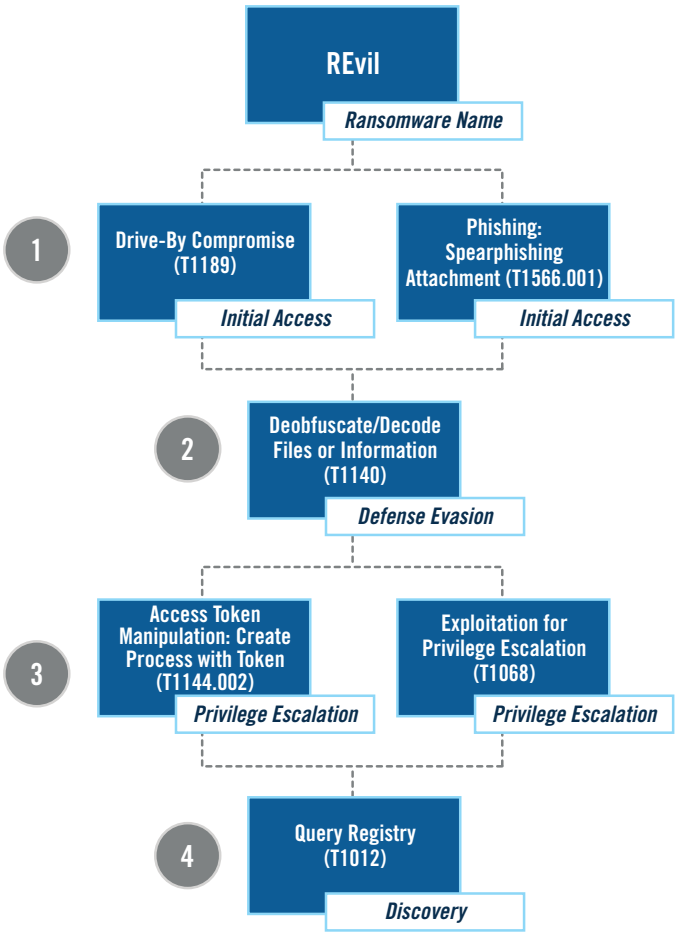
- In June 2021, the healthcare giant Grupo Fleury was targeted by REvil operators; their systems became unavailable, and they had to work to restore services. (Abrams, 2021)
- In April 2020, a California-based COVID-19 research firm, 10x Genomics, was targeted in a massive hack by REvil operators, who stole 1 TB of data and posted parts of it online. (Davis, Another COVID-19 Research Firm Targeted by Ransomware Attack, 2020)
- In 2020, REvil operators stole data from a large cosmetic surgery chain used by celebrities called the Hospital Group. They obtained 900 GB of photos and threatened to leak and publish before-and-after photos, as well as other details, if the ransom was not paid. (Tidy, 2020)
- In August 2020, REvil ransomware operators breached Valley Health systems and claimed to be in possession of company private data, client and employee details, and snapshots of folders. They released a small portion of the leak, which contained patient prescriptions, personal details of patients, medical scan reports, digital imaging and communication medical files, and more. (cybleinc, 2020)
- In November 2019, REvil operators compromised a remote administration tool used to configure and troubleshoot client offices at Complete Technology Solutions, an IT service vendor for dental practices. The attack spread to at least 100 dentistry businesses. Many businesses had to turn away patients until the system outages could be handled. (Davis, Ransomware Hits Another IT Vendor, Impacting 100 Dental Providers, 2019)

REvil Timeline of Techniques

The following is a composite timeline of the REvil ransomware behavior, derived from public threat reporting of REvil via five different vendors (Secureworks, Intel471, McAfee, Blackberry, and Picus) outlined in Appendix A of the full document. In the following charts, parallel boxes represent one or more behaviors that the malware might perform in a given penetration. It is possible that for any given breach, the REvil deployment in question will perform one or many behaviors.

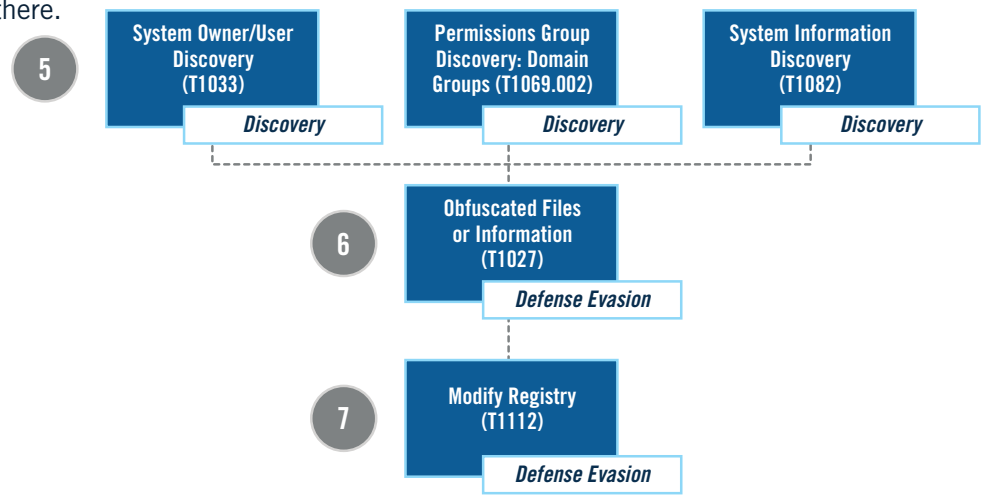
Initial Access to Victim's Environment

Before REvil can begin to infect a machine, it must first gain access to the environment. What made REvil so damaging from its start in 2019 was that its operators leveraged a wide variety of methods for gaining access to a victim's machine. Among some of the techniques were *Drive-By Compromise* [T1189] and *Spearphishing Attachment* [T1566.001]. Once it has achieved control of a system, REvil needs to *Deobfuscate/Decode Files or Information* [T1140] for its own data and configuration. Once decrypted, the software has been observed using the *Exploitation for Privilege Escalation* [T1068] technique, which involves exploiting known common vulnerabilities and exposures (CVE) vulnerabilities. When the malware is not using these, it may create a process with tokens to elevate privileges. This allows REvil to gain higher privileges to perform more sophisticated tasks.



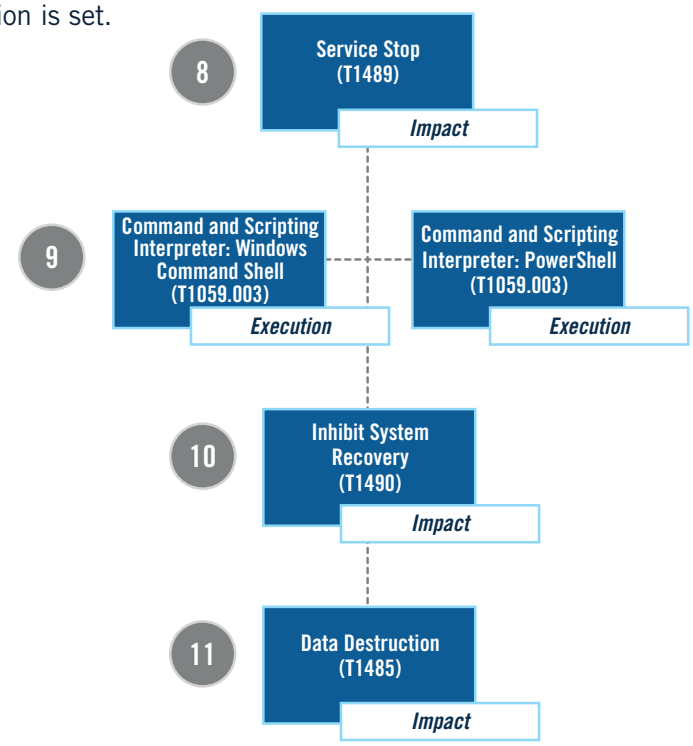
Profiling Host Information

When REvil has made its way on to a system, the software must search and collect a few host items via System Information Discovery [T1082], Domains Groups [T1069.002], and System Owner/User Discovery [T1082] to aid in encryption. Once it has finished gathering the information it needs, the software encrypts that data (Obfuscated Files or Information [T1027]) and changes the Windows Registry [T1112] by storing this information there.



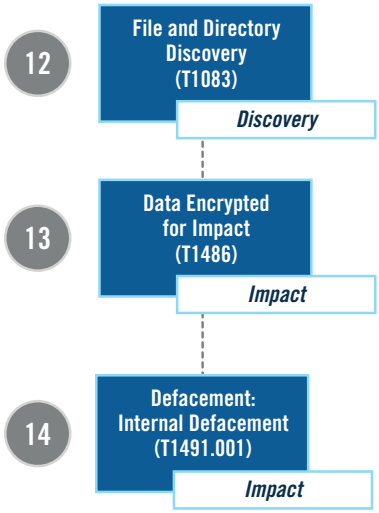
Preparing for Encryption Process

To prepare for the encryption process, REvil will stop any necessary services that prevent encryption from a preconfigured list. The malware will then either open the Windows Command Shell [T1059.003] or PowerShell [T1059.001] prompt to perform Inhibit System Recovery [T1490] and Data Destruction [T1485] techniques. Once this task is done, the malware has the option to wipe the data from the system if a certain flag within its configuration is set.



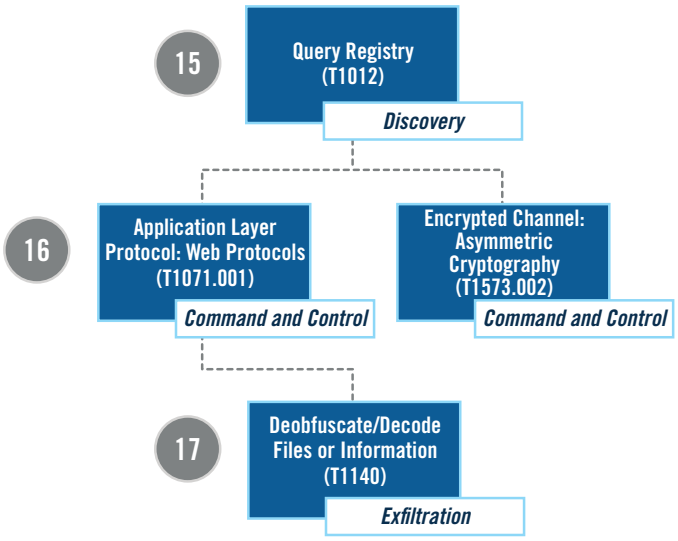
Encryption Process Begins

REvil will first perform a File and Directory Discovery [T1083] search on the system to determine which files to include or exclude for encryption. Then it will start to encrypt the data (Data Encrypted for Impact) [T1486]. Once the encryption is complete, the malware will internally deface the victim's machine by changing the desktop background to an intimidating wallpaper (Defacement: Internal Defacement) [T1491.001].



Post-Encryption Process

First, REvil will check the Registry (Query Registry [T1012]) to see if a specific flag is set in the configuration (the "net" value is set to "True"). Then REvil will initiate an Encrypted Channel: Asymmetric Cryptography [T1573.002] for command and control (C2) over Hypertext Transfer Protocol Secure (HTTPS), which is considered Web Protocols [T1071.001]. It does not rely on network communication, but the malware is capable of Exfiltration over C2 Channel [T1041] to take the data out of the victim's environment if the opportunity presents itself or is needed.



Composite Table

The following is a combined table of techniques commonly observed in use by REvil. For a detailed accounting of the techniques and procedure examples and source references from each public threat reporting source beyond what is listed below, please see **Appendix A** of the full paper. It is also important to note that these techniques are not necessarily executed in exact order by REvil operators.

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	TECHNIQUE DESCRIPTION	PROCEDURE EXAMPLE(S)
initial access	T1189	drive-by compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing.	Elevate privileges using Local Privilege Escalation (LPE) exploit if this key is enabled, CVE-2018-8453 exploited.
initial access	T1566.001	spearphishing attachment	Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems.	Spam emails with attached MS Office Word documents including malicious macro to download ransomware to target system.
execution	T1204.001	user execution: malicious file	An adversary may rely upon a user opening a malicious file in order to gain execution.	Lures victim into clicking to enable content that launches the code hidden in macros.
privilege escalation	T1068	exploitation for privilege escalation	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.	Attempts to run with elevated privileges by exploiting CVE-2018-8453 vulnerability to gain SYSTEM privileges on host.
discovery	T1012	query registry	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.	Checks the Registry to see if it has already generated and stored session encryption keys, and does another check to the Registry to confirm whether C2 communication should take place.
privilege escalation	T1134.002	access token manipulation: create process with token	Adversaries may create a new process with a duplicated token to escalate privileges and bypass access controls.	Verifies that it is running with administrative rights via making sure that TokenElevationType is set to TokenElevationTypeFull and its integrity level is set to a minimum level of High. However, if it is running with low integrity, it will use the RunAs command to relaunch a new instance of itself with administrative rights.

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	TECHNIQUE DESCRIPTION	PROCEDURE EXAMPLE(S)
discovery	T1082	system information discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.	REvil will continue to profile and search for hostname, fixed drive details, central processing unit (CPU) architecture, keyboard layout information, volume serial number for system drive, and the operating system product name.
defense evasion	T1027	obfuscated files or information	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.	Has obfuscated user profile information, modules/ functions, and will encrypt components from the configuration data stored in the Registry. All strings have also been encrypted with RC4 before use.
discovery	T1033	system owner User discovery	Adversaries may attempt to identify the primary user, currently logged-in user, set of users that commonly uses a system, or whether a user is actively using the system.	REvil will also collect the current username from the victim's machine.
discovery	T1069.002	permissions groups discovery: domain groups	Adversaries may attempt to find domain-level groups and permission settings.	REvil will also search the workgroup to collect domain group information.
defense evasion	T1112	modify registry	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.	REvil stores encrypted system information added to the Registry. It will check if it is already generated and stored the session encryption keys in the victim's Registry. The "Software\recfg" Registry subkey can indicate that REvil has infected the system, so monitoring around this subkey can help with detection.

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	TECHNIQUE DESCRIPTION	PROCEDURE EXAMPLE(S)
impact	T1489	service stop	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.	REvil will stop and delete services if name matches list of service in JavaScript Object Notation (JSON) config list; these are potential resources that can conflict or impede REvil's ability to wipe or encrypt files. Also has terminated all processes specified by prc value.
impact	T1490	inhibit system recovery	Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.	REvil has been seen to destroy all shadow volumes of the victim machine and disable protection of the recovery boot with this command: exe /c vssadmin. exe Delete Shadows / All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures.
execution	T1059.003	command and scripting interpreter: windows command shell	Adversaries may abuse the Windows command shell for execution.	REvil has used cmd.exe to perform inhibit system recovery technique.
impact	T1485	data destruction	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources.	If flag is set to True, all the files and folders listed under wfld will be zeroed out and deleted with random trash or NULL values.
discovery	T1083	file and directory discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.	REvil has iterated through all folders and files residing on local fixed drives and verifies they are not included in config lists and has an exclude list as well.

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	TECHNIQUE DESCRIPTION	PROCEDURE EXAMPLE(S)
impact	T1486	data encrypted for impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.	REvil has used multithreading I/O completion ports and encrypts files simultaneously as well as the Salsa2.0 algorithm. It will encrypt the flagged files and drop a ransom note in each folder.
impact	T1491.001	defacement: internal defacement	An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users.	After encryption, REvil will create a bitmap image of the desktop in runtime with the text that comes with the config file prepared with the random extension and set this and the ransom note to the desktop background. The text will read "You are infected!" and it will explain where the user can go to read. instructions in the text file on the system
command and control	T1071.001	application layer protocol: web protocols	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/ network filtering by blending in with existing traffic.	if the "net" key is set to "true" then it will communicate with the C2 server via POST messages (to a list of domains in the config file) to send information using the HTTPS protocol; this is an optional functionality for REvil.
exfiltration	T1041	exfiltration over C2 channel	Adversaries may steal data by exfiltrating it over an existing C2 channel.	REvil has sent host profile and malware information to C2 Uniform Resource Locator (URL) via the HTTP POST method.
command and control	T1573.002	encrypted channel: asymmetric cryptography	Adversaries may employ a known asymmetric encryption algorithm to conceal C2 traffic rather than relying on any inherent protections provided by a communication protocol.	If flag is set, it will conceal C2 communications using an asymmetric key scheduling algorithm.

REvil's Tactics, Techniques, and Procedures

Section 3 of the full document goes into detail about every technique listed under REvil and how it was used for ransomware purposes. Each technique is organized by the tactic level and can be found under the relevant tactic heading.

The following is a listing of the tactics, techniques, and procedures (TTPs) covered by the ransomware variant REvil. For ransomware, each of the technique's procedure examples might be used in a unique way that helps contribute to the attacker's goals of locking the machine and getting the ransom from the victim.

Initial Access

- aT1189 Drive-by Compromise
- T1566.001 Phishing: Spearphishing Attachment

Discovery

- T1082 System Information Discovery
- T1083 File and Directory Discovery
- T1007 System Service Discovery
- T1012 Query Registry
- T1069.002 Permission Groups Discovery: Domain Groups

Defense Evasion

- T1036.005 Masquerading: Match Legitimate Name or Location
- T1562.001 Impair Defenses: Disable or Modify Tools

Privilege Escalation

- T1068 Exploitation for Privilege Escalation
- T1134.002 Access Token Manipulation: Create process with Token

Execution

- T1047 Windows Management Instrumentation
- T1059.001 PowerShell
- T1059.003 Windows Command Shell
- T1059.005 Visual Basic
- T1106 Native API
- T1204.002 User Execution: Malicious File

Command and Control

- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1573.002 Asymmetric Cryptography

Exfiltration

- T1041 Exfiltration over C2 Channel

Impact

- T1490 Inhibit System Recovery
- T1489 Service Stop
- T1486 Data Encrypted for Impact
- T1485 Data Destruction
- T1491.001 Internal Defacement

REvil's TTP Detection and Mitigations

The final section, Section 4, of the paper goes through the detection analytics and mitigation strategies for each of the TTPs observed by REvil in public threat reporting.

Section 4.1 covers the analytics strategy to explain how a security team can implement and prioritize behavioral analytics.

Section 4.2 is outlined in the full document and can be referenced for more detail:

4.2.1 General preparation

- Establishing procedures, threat assessment, and establishing baseline behaviors

4.2.2 Incident response process preparation

- Creating an incident response team and ransomware response plan

4.2.3 Incident recovery

- Having a disaster recovery plan in place

4.2.4 Recommendations for smaller organizations

- Advice for organizations that lack subject matter experts or have limited resources for defense

Section 4.3 includes responses to specific techniques that encompass the following:

- Each individual technique and corresponding detection and mitigations are covered.
- Threat detection overview for each technique; this includes the general detection description from ATT&CK as well as any additional analytics from MITRE's Cyber Analytics Report or Sigma that can be relevant to finding and detecting these techniques.
- Mitigations are referenced from ATT&CK's resources, including the appropriate mitigation ID, name, and description

References/Bibliography

1. Abrams, L. (2021, 06 23). *Healthcare giant Grupo Fleury hit by REvil ransomware attack*. Retrieved 07 21, 2021, from https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil-ransomware-attack/
2. Checkpoint. (2020, 10 29). *Hospitals Targeted in Rising Wave of Ryuk Ransomware Attacks - Check Point Software*. Retrieved 07 21, 2021, from https://blog.checkpoint.com/2020/10/29/hospitals-targeted-in-rising-wave-of-ryuk-ransomware-attacks/
3. Cybleinc. (2020, 08 27). *REvil Allegedly Targets Another Healthcare Organization*. Retrieved 07 21, 2021, from REvil Allegedly Targets Another Healthcare Organization
4. Davis, J. (2019, 12 09). *Ransomware Hits Another IT Vendor, Impacting 100 Dental Providers*. Retrieved 07 21, 2021, from https://healthitsecurity.com/news/ransomware-hits-another-it-vendor-impacting-100-dental-providers
5. Davis, J. (2020, 04 08). *Another COVID-19 Research Firm Targeted by Ransomware Attack*. Retrieved 07 21, 2021, from https://healthitsecurity.com/news/another-covid-19-research-firm-targeted-by-ransomware-attack
6. MITRE. (2021). *MITRE ATT&CK*. (MITRE) Retrieved 07 21, 2021, from https://attack.mitre.org/
7. Program, H. C. (2021, June 3). *Ransomware Trends 2021*. Retrieved June 23, 2021, from https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
8. Strom, B. A. (2020, 03). *Microsoft Word - ATTACK Design and Philosophy subs revision v1.2.docx*. Retrieved 07 21, 2021, from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
9. Tidy, J. (2020, 12 24). *Hackers threaten to leak plastic surgery pictures*. Retrieved 07 21, 2021, from https://www.bbc.com/news/technology-55439190
10. Waldman, A. (2020, 04 03). *Microsoft warns hospitals of impending ransomware attacks*. Retrieved 07 21, 2021, from https://searchsecurity.techtarget.com/news/252481164/Microsoft-warns-hospitals-of-impending-ransomware-attacks
11. Secureworks. (2019, 11, 24). *REvil/Sodinokibi Ransomware*. Retrieved 10 18, 2021, from https://www.secureworks.com/research/revil-sodinokibi-ransomware

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®