
# RANSOMWARE GETTING STARTED GUIDE AND DEEP DIVE INTO REvil

Jaclyn Lasky, Chris Naughton, Pete McPherson, Eric Arnoth, and Connie Zhang

 #21-3872 8-10-2022

## Abstract

This paper goes into detail about the REvil ransomware variant and its operators to provide an in-depth look at how it begins its infection chain and why. The paper also covers publicly available information on REvil's cyber-attacks that targeted industries in the healthcare sector, and why it matters. The paper consists of two main parts. **Sections 2 and 3** document the REvil malware's operation in the flow of a typical operation, based upon observations documented in the MITRE ATT&CK® Framework, additional public threat reporting, and some internal analysis in the MITRE Lab. **Section 4** reviews these adversary behaviors from the perspective of a defender, giving guidance on how cyber practitioners could detect and protect against such a threat.

# Executive Summary

This paper is intended to assist institutions within the healthcare sector to understand and defend against ransomware attacks. It includes an overview of ransomware, provides a detailed narrative of its typical order of operation, details its potential impact on institutions within the healthcare sector, and furnishes some guidance on defending before and during an attack. To achieve this, it leverages the MITRE ATT&CK Framework to provide a structured view of the behavior of the malware and its operators, detailing the tactics, techniques, and procedures (TTPs) used. Specifically, it presents the REvil [S0496] ransomware variant and its typical behaviors will be presented for consideration, along with a guide for getting started with threat detection of ransomware activity. The paper also leverages other resources for the defensive guidance offered, such as the MITRE Cyber Analytics Repository (CAR), as well as other such sources. Although written with the healthcare sector in mind, the technical details provided here should mostly be applicable to other ransomware attacks in other industries.

## Intended Audience

This document is primarily intended to be used by cybersecurity and information technology professionals who need to protect their institutions against ransomware attacks and to provide the earliest possible detection if an attack should occur.

## How to Use This Document

Each section of this document is intended to assist members of an organization to gain a better understanding of all aspects of a ransomware attack so they are better equipped to identify and defend against it.

- **Section 1: Introduction** provides details about ransomware and its impact on an organization.
- **Section 2 REvil Sequence of Adversary Actions** provides timeline details of a ransomware attack involving the REvil variant.
- **Section 3: Detailed REvil Tactics, Techniques, and Procedures** details the specific TTPs utilized by REvil to attack an organization.
- **Section 4: Ransomware Mitigations and Detections** offers suggestions for mitigations and detections that can be put in place to improve the security posture of an organization, as well as advice on what should be in place to defend against an attack.
- **Section 5: References** includes the references that were used to create the content of this document.

# Table of Contents

**Introduction . . . 1**
- Ransomware Introduction . . . 1
  - Impact on Healthcare Sector . . . 1
  - Technology and Risk . . . 1
- Preparation . . . 2
- Evaluate the Situation . . . 2
  - Handling the Ransom . . . 2
  - Detection for Ransomware . . . 2
- MITRE ATT&CK . . . 3
  - Encryption Process Begins . . . 4
- REvil . . . 5
  - Impact on the Health Sector . . . 5
  - Characteristics . . . 5
  - Adversary Groups Using REvil Ransomware . . . 6

**REvil Sequence of Adversary Actions . . . 7**
- Initial Access to Victim's Environment . . . 7
- Profiling Host Information . . . 8
- Preparing for Encryption . . . 8
- Encryption Process Begins . . . 9
- Post-Encryption Process . . . 9

**Detailed REvil Tactics, Techniques, and Procedures . . . 14**
- Initial Access . . . 15
  - T1189 Drive-by Compromise . . . 15
  - T1566.001 Phishing: Spearphishing Attachment . . . 15
- Discovery . . . 15
  - T1082 System Information Discovery . . . 15
  - T1083 File and Directory Discovery . . . 15
  - T1007 System Service Discovery . . . 15
  - T1012 Query Registry . . . 15
  - T1069.002 Permission Groups Discovery: Domain Groups . . . 15

Defense Evasion . . . 15
T1036.005 Masquerading: Match Legitimate Name or Location . . . 15
T1562.001 Impair Defenses: Disable or Modify Tools . . . 15
Privilege Escalation . . . 15
T1068 Exploitation for Privilege Escalation . . . 15
T1134.002 Access Token Manipulation: Create Process with Token. . . . 15
Execution . . . 15
T1047 Windows Management Instrumentation . . . 15
T1059.001 PowerShell . . . 15
T1059.003 Windows Command Shell . . . 15
T1059.005 Visual Basic . . . 15
T1106 Native API . . . 15
T1204.002 User Execution: Malicious File . . . 15
Command and Control . . . 15
T1071.001 Web Protocols . . . 15
T1105 Ingress Tool Transfer . . . 15
T1573.002 Asymmetric Cryptography . . . 15
Exfiltration . . . 15
T1041 Exfiltration Over C2 Channel . . . 15
Impact . . . 15
T1489 Service Stop . . . 15
T1490 Inhibit System Recovery . . . 15
T1486 Data Encrypted for Impact . . . 15
T1491.001 Defacement: Internal Defacement. . . . 15
T1486 Data Destruction . . . 15
Initial Access . . . 15
T1189 Drive-by Compromise. . . . 15
T1566.001 Phishing: Spearphishing Attachment . . . 16

Discovery . . . . . . . . . . 16
T1082 System Information Discovery . . . . . . . . . . 16
T1083 File and Directory Discovery . . . . . . . . . . 16
T1007 System Service Discovery . . . . . . . . . . 17
T1012 Query Registry . . . . . . . . . . 18
T1069.002 Permission Groups Discovery: Domain Groups . . . . . . . . . . 18
Defense Evasion . . . . . . . . . . 18
T1036.005 Masquerading: Match Legitimate Name or Location . . . . . . . . . . 18
T1562.001 Impair Defenses: Disable or Modify Tools . . . . . . . . . . 18
T1070.004 Indicator Removal on Host: File Deletion . . . . . . . . . . 19
T1027 Obfuscated Files or Information . . . . . . . . . . 19
T1055 Process Injection . . . . . . . . . . 19
T1134.001 Access Token Manipulation: Token Impersonation/Theft . . . . . . . . . . 19
T1140 Deobfuscate/Decode Files or Information . . . . . . . . . . 19
T1112 Modify Registry . . . . . . . . . . 20
Privilege Escalation . . . . . . . . . . 20
T1068 Exploitation for Privilege Escalation . . . . . . . . . . 20
T1134.002 Access Token Manipulation: Create Process with Token . . . . . . . . . . 21
Execution . . . . . . . . . . 21
T1047 Windows Management Instrumentation . . . . . . . . . . 21
T1059.001 PowerShell . . . . . . . . . . 21
T1059.003 Windows Command Shell . . . . . . . . . . 21
T1059.005 Visual Basic . . . . . . . . . . 21
T1106 Native API . . . . . . . . . . 21
T1204.002 User Execution: Malicious File . . . . . . . . . . 21
Command and Control . . . . . . . . . . 22
T1071.001 Web Protocols . . . . . . . . . . 22
T1105 Ingress Tool Transfer . . . . . . . . . . 23
T1573.002 Asymmetric Cryptography . . . . . . . . . . 23
Exfiltration . . . . . . . . . . 23
T1041 Exfiltration over C2 Channel . . . . . . . . . . 23

Impact . . . 24
T1489 Service Stop . . . 24
T1490 Inhibit System Recovery . . . 25
T1486 Data Encrypted for Impact . . . 25
T1491.001 Defacement: Internal Defacement . . . 26
T1486 Data Destruction . . . 26
**Ransomware Mitigations and Detections . . . 27**
Analytics Strategy . . . 27
Defensive Strategy . . . 28
General Preparation . . . 28
Incident Response Process Preparation . . . 28
Incident Recovery . . . 28
Recommendations for Smaller Organizations . . . 29
**Responses to Specific Techniques . . . 30**
**Conclusion . . . 53**
**References . . . 54**
**Appendix A: REvil Technique Timelines from Public Threat Reporting . . . 55**

## List of Figures

Figure 1. Initial Access to Victim's Environment . . . . . . . . . . . . . . . . . . . . . . . . 7
Figure 2. Gathering Information from the Host Machine . . . . . . . . . . . . . . . . . . . . 8
Figure 3. Performing Behaviors Necessary for Encryption . . . . . . . . . . . . . . . . . . . . 8
Figure 4. Encryption Process . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
Figure 5. Post-Encryption Process and C2 Communication . . . . . . . . . . . . . . . . . . . 9
Figure 6. ATT&CK Navigator View of REvil's Techniques . . . . . . . . . . . . . . . . . . . 14
Figure 7. REvil Performing File Searching on the System . . . . . . . . . . . . . . . . . . . 17
Figure 8. Registry Modifications Made by REvil in the MITRE Lab . . . . . . . . . . . . . . . 20
Figure 9. Ransom Note Dropped by REvil to Victim's Machine that Details How to Pa the Ransom . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
Figure 10. REvil Has Encrypted the System Files and Changed the Desktop Wallpaper to Notify and Intimidate the User . . . . . . . . . . . . . . . . . . . 26

## List of Tables

Table 1. Composite Table . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

# 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, this has the potential to translate into lost lives of the patients in the care of an impacted institution.

## Ransomware Introduction

Ransomware is malicious software that compromises computer systems, renders data inaccessible, and prevents use of the affected systems. A demand for ransom is then delivered to the legitimate users of the system, with the promise of restoring system operation and data access upon payment. Another resource to look at is the Evolution of Ransomware paper that was written by MITRE to detail how ransomware has grown to where it is and how the impact has changed over time to produce larger implications in the healthcare sector and others.

### Impact on Healthcare Sector

Hospitals and other healthcare institutions have become a target by adversaries for many reasons. These institutions need to return to normal operations as quickly as possible, in order to respond to medical emergencies and save lives. As such, the ransom is more likely to be paid in a timely fashion than if the target organization belonged to a different industry. Many of the targeted institutions in the sector are small to mid-range. This size organization often lacks dedicated cybersecurity staff, and the information technology (IT) staff serves in that capacity, in addition to building and maintaining the IT systems needed for day-to-day operations.

### Technology and Risk

The technology environment in most healthcare institutions also has a multitude of embedded devices and operational technology (OT) systems that are tied to the IT systems breached by ransomware operators, such as medical test equipment, drug delivery systems, telemedicine tools, and so forth. These 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. Impacting these OT systems together with an already overburdened IT staff can be catastrophic, resulting in disruption of patient care and loss of life.

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. Protected Health Information often resides on such equipment, meaning a breach can result in data privacy issues. From a regulatory standpoint, the primary concern for healthcare institutions is HIPAA compliance, but to avoid negative outcomes to patients, the data needs to be safeguarded against breach.

When ransomware has infected a network, it can severely impact all these areas, and has been observed not only to target services to impact availability of this information, but also to exfiltrate the sensitive data of patients in an effort to inflict even more damage.

## Preparation

Ultimately, the best defense against ransomware's impact is for an organization to have resilient means of operation in the case of an attack; additional details for preparation can be found in the "Incident Preparedness and Response" paper. At a minimum, this will mean a robust facility for backing up all critical data. Backups of data should be performed automatically and stored offline, detached from the computer systems that normally store and processes the information in question. Restoration of backup data should be tested regularly, and the backup process should be validated on an ongoing basis.

There are means to help mitigate ransomware attacks as they occur. The best place to start is by looking at what data the organization is collecting; by doing this, gaps in coverage can be identified. If an organization has a Data Privacy officer, that individual should be involved in response planning . Once the data in the organization's environment is understood, then open-source analytics like Sigma or MITRE CAR can be utilized. There are also analytic references available at Deploy Cyber Analytics I Health Cyber: Ransomware Resource Center (mitre.org).(See 4 Ransomware Mitigations and Detections).

Having regular backups for data is important, but detecting an attack as early as possible is also critical. In addition to backups and planning, it is also helpful to consider cyber insurance to cover ransomware ransoms and impact, and for conducting negotiations.

Additionally, alternative means to operate without primary computer systems may be appropriate. This may mean using secondary, alternative computer systems and networks, though to be truly effective as an alternative, those secondary systems would need to be separated from the primary network by an air gap. Paper alternatives where possible may be the best means to conduct some operations without the primary computer systems, but this may not be possible in many circumstances.

## Evaluate the Situation

When an incident occurs, the first step is to recognize what is going on and look toward any plans that were developed ahead of time. Once this is addressed, then the next step would be to examine assets and configurations. Any device that is intelligent and can connect to the network may be vulnerable, so all types of hospital equipment need to be reviewed and confirmed to be following best security practices. Any security plans that are in development need to take inventory of all types of devices that are available (e.g., medical devices, monitoring devices, tablets, etc.).

### Handling the Ransom

A question that many victims face is "Do I pay the ransom?" MITRE is not fit to advise what each individual organization should decide. The federal government guidance is that paying the ransom is a business decision, but payment does not guarantee data will be recovered or that it will be protected from further attacks. (Dept of Treasury, 2021) Enabling a plan for this occurrence can help organizations understand risks, budget, stability of backups, and risk of data being leaked, and take measures to implement the best detection capabilities possible to avoid the worst case scenario. Evaluate which endpoints or systems are more at risk if disrupted or destroyed, and which ones are less risk and can go without paying the ransom for. For more guidance, see the Crown Jewels Analysis (CJA) paper in the ransomware resource center. If the conversations are had before (not after) a ransomware situation occurs, it will be a lot easier to make those decisions as efficiently as possible, especially as time can be critical in hospitals or other healthcare facilities where operations cannot risk being ceased. Having a ransomware response and action plan will help ensure the best possible outcome when deciding to either pay or not pay the ransom.

### Detection for Ransomware

Detection should be similar across many industries and organizations. The healthcare industry has its own set of specific needs and unique types of equipment that affect data collection. At the same time, ransomware will behave in a similar fashion across sectors, except for any variants that target healthcare specifically.

Based on the sophistication of the organization, several starting points for detection exist. Two types of detection are Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs)-Based Detection.

An easy starting point is to review IOCs. They are relatively easy to detect but provide limited benefits, since they are typically easily changed by adversaries. IOCs are things like Internet Protocol addresses, domains, file hashes, and filenames that can be associated with malicious activity.

More advanced characterization of malicious activity looks toward identifying what TTPs the adversary may use. The next section will focus on what techniques REvil uses, and after that it will cover detection and mitigations for those specific techniques. Walking through one ransomware sample for an organization that is a likely target of these types of attacks will not be enough. For the case of REvil, the behaviors publicly documented will be listed and reviewed.

Evaluating a specific ransomware and the adversaries that utilize it can provide defenders with a concrete example to understand how other, similar malware will behave.

## MITRE ATT&CK

The MITRE ATT&CK Framework will be used extensively throughout this paper to provide a structured review and analysis of the malware to be examined. The MITRE ATT&CK Framework is "a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." (MITRE, 2021) The MITRE ATT&CK Framework documents adversary behaviors to better enable defenders to know how to detect and defend. The content in the framework is derived from publicly available cyber threat intelligence (CTI) by third parties that documents observed behaviors and tools used by adversaries in actual breaches and campaigns.

As detailed in the *MITRE ATT&CK Philosophy Guide* (Strom, 2020), the general structure of MITRE ATT&CK is as follows (definitions below are quoted from the Guide):

- **Techniques** represent "how" an adversary achieves a tactical objective by performing an action. Each Technique has a unique ID, in the format T###.
- **Sub-techniques** further break down behaviors described by techniques into more specific descriptions of how behavior is used to achieve an objective. Each Sub-technique has a unique ID, in the format T###.###.
- **Procedure Examples** are the specific implementation adversaries have used for techniques or sub-techniques.
- **Tactics** represent the "why" of an ATT&CK technique or sub-technique. Each Tactic has a unique ID, in the format TA####.

- **Groups** Known adversaries that are tracked by public and private organizations and reported on in threat intelligences reports are tracked within ATT&CK under the Group object. Groups are defined as named intrusion sets, threat groups, actor groups, or campaigns that typically represent targeted, persistent threat activity. Each Group entry has a unique ID, in the format G####.
- **Software** Adversaries commonly use different types of software during intrusions. Software can represent an instantiation of a technique or sub-technique, so they are also necessary to categorize within ATT&CK for examples on how techniques are used. Software is broken out into two high-level categories: tools and malware. (pg 14) Each Software entry has a unique ID, in the format S###.

All MITRE ATT&CK Techniques, Sub-techniques, Tactics, Groups, and Software are documented publicly on attack.mitre.org and will be linked directly when referenced in this document.

## Encryption Process Begins

One of the key aspects of the MITRE ATT&CK Framework is the concept of Tactics, which give a short-term, tactical reason for an adversary behavior documented in a Technique and/or Sub-technique. This document will use ATT&CK Tactics to present the narration of the ransomware order of operation.

While this presentation will convey a given sequence based on analysis of the observations by the CTI used by ATT&CK to document REvil, it is important to note that more broadly speaking, adversaries may operate very differently. Achieving given tactical objectives in an advanced adversary campaign is not a consistently linear progression. The adversary will cycle through tactical objectives using various techniques tailored to the circumstances at the time to achieve their long-term objectives.

Here is a short summary of all the Tactics in MITRE ATT&CK. The descriptions below are quoted directly from the Framework's website.

- *Reconnaissance* [TA0043]: The adversary is trying to gather information they can use to plan future operations.
- *Resource Development* [TA0042]: The adversary is trying to establish resources they can use to support operations.
- *Initial Access* [TA0001]: The adversary is trying to get into a network.
- *Execution* [TA0002]: The adversary is trying to run malicious code.
- *Persistence* [TA0003]: The adversary is trying to maintain their foothold.
- *Privilege Escalation* [TA0004]: The adversary is trying to gain higher-level permissions.
- *Defense Evasion* [TA0005]: The adversary is trying to avoid being detected.
- *Credential Access* [TA0006]: The adversary is trying to steal account names and passwords.
- *Discovery* [TA0007]: The adversary is trying to figure out the environment.
- *Lateral Movement* [TA0008]: The adversary is trying to move through the environment.
- *Collection* [TA0009]: The adversary is trying to gather data of interest to their goal.
- *Command and Control* [TA0011]: The adversary is trying to communicate with compromised systems to control them.
- *Exfiltration* [TA0010]: The adversary is trying to steal data.
- *Impact* [TA0040]: The adversary is trying to manipulate, interrupt, or destroy the systems and data

## REvil

This paper will use REvil [S0496] as a case study for an example ransomware attack. REvil is a ransomware-as-a-service (RaaS) variant that has been in use by the GOLD SOUTHFIELD [G0115] group since at least April 2019. The software has additional aliases, such as Sodin and Sodinokibi. Aliases are important to note because adversaries can try to change the name of their malware to conceal operations and avoid names that cybersecurity practitioners know to be malicious. REvil operators have been going on and offline due to increased law enforcement pressure on ransomware operators. (Vaas, 2021)

### Impact on the Health Sector

Adversaries using REvil have targeted the healthcare sector on many occasions in recent years.

- 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, where they 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 wasn't 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)

### Characteristics

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 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.

### Adversary Groups Using REvil Ransomware

REvil has been seen used by the GOLD SOUTHFIELD adversary group. They are a financially motivated group that has been active since at least 2019.

When looking at mitigations and detections for specific techniques for ransomware, the groups should also be considered as a place to start for writing analytics. The techniques used by the group that is using the ransomware might also show up in the compromised environment, and therefore should also be considered.

## REvil Sequence of Adversary Actions

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. 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.

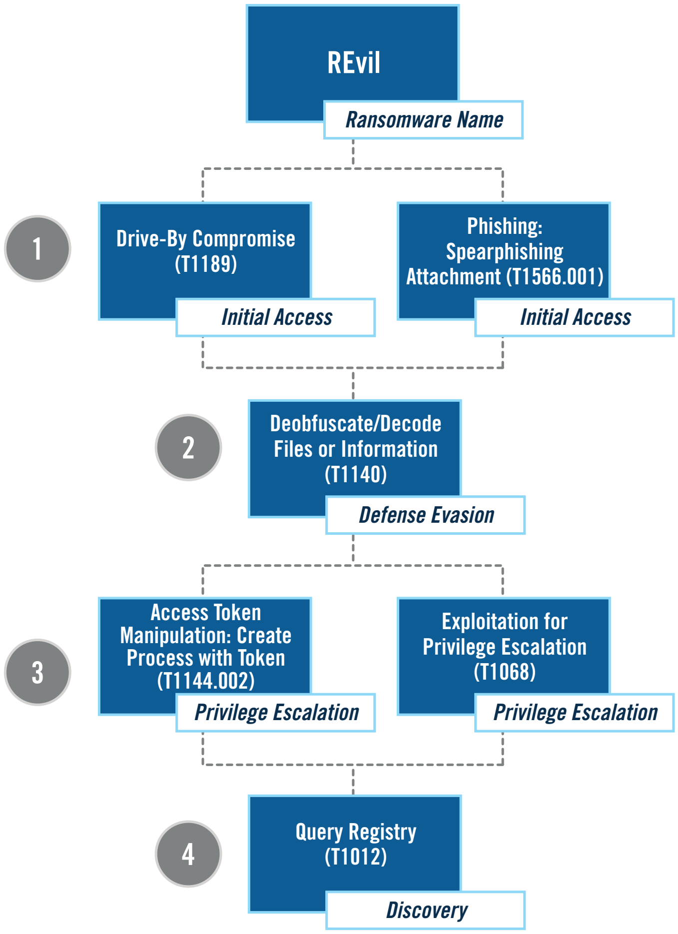


**FIGURE 1: INITIAL ACCESS TO VICTIM'S ENVIRONMENT**

## 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.

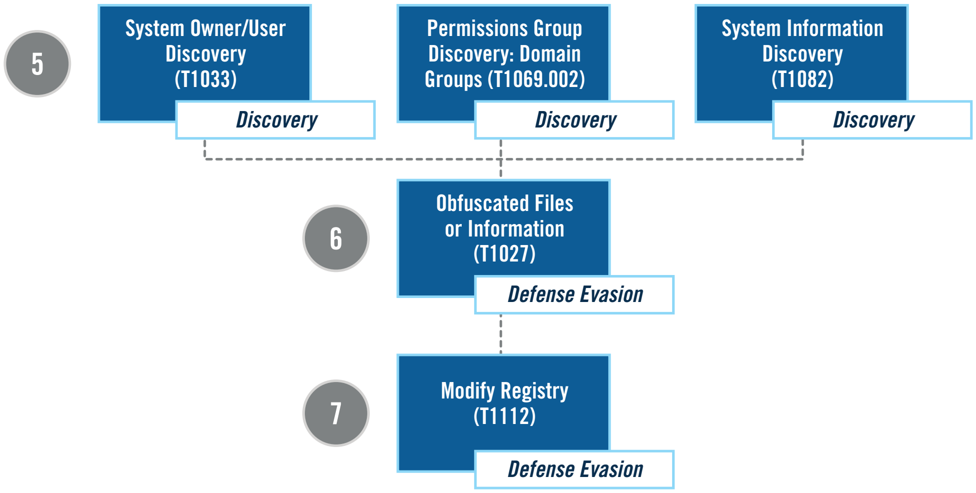


FIGURE 2: GATHERING INFORMATION FROM THE HOST MACHINE

## Preparing for Encryption

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.

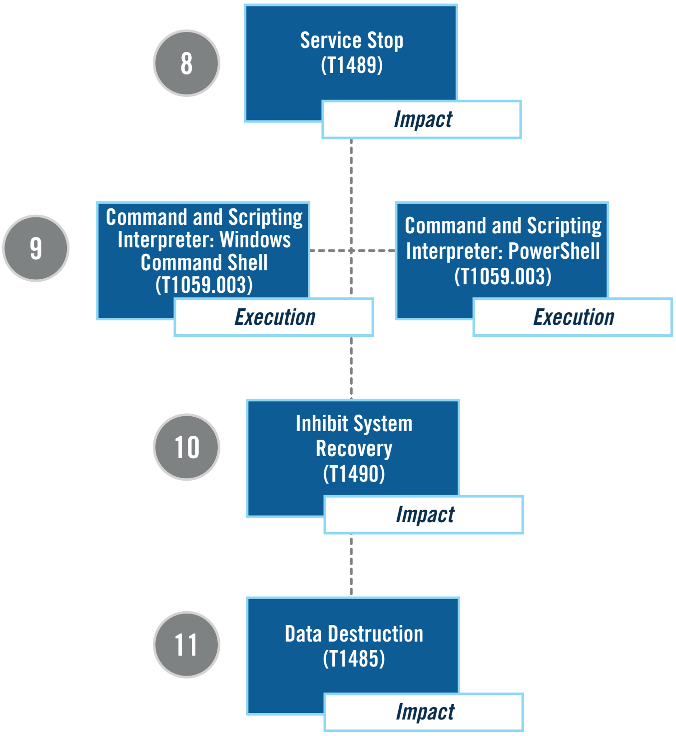


FIGURE 3: PERFORMING BEHAVIORS NECESSARY FOR ENCRYPTION

## 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]

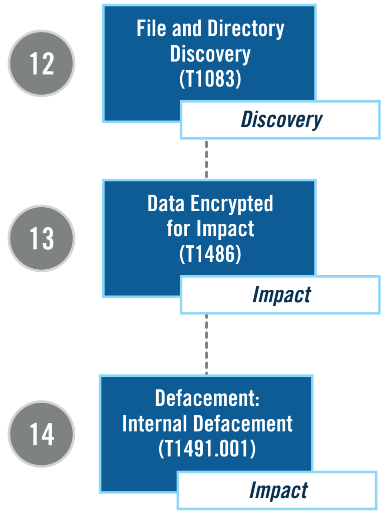


**FIGURE 4: ENCRYPTION PROCESS**

## 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.

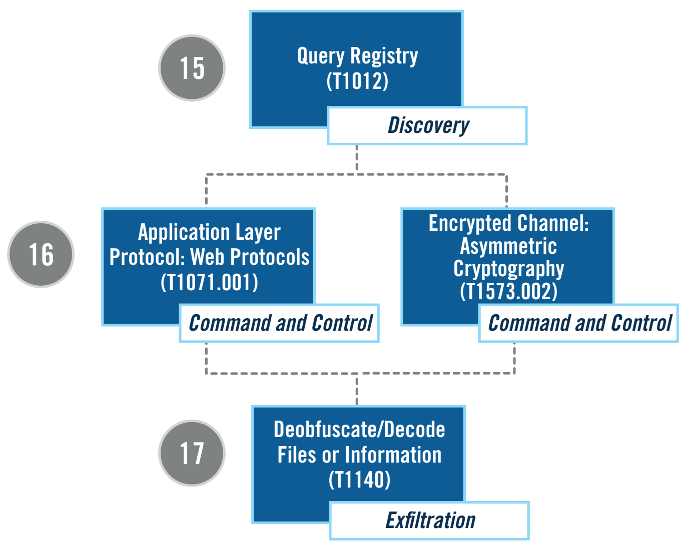


**FIGURE 5: POST-ENCRYPTION PROCESS AND C2 COMMUNICATION**

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**. It is also important to note that these techniques are not necessarily executed in exact order by REvil operators.

**TABLE 1. COMPOSITE TABLE**

| 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.<br><br>It will check if it is already generated and stored the session encryption keys in the victim's Registry.<br><br>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. |

# Detailed REvil Tactics, Techniques, and Procedures

This section will further investigate the main set of techniques that are exhibited by the REvil ransomware, as documented in MITRE ATT&CK. This section will provide a narrative to present the TTPs used by REvil, showing the context of its behavior during the course of a typical campaign, meaning these techniques have been counted and averaged across five different REvil scenarios from public threat reporting.

Using the ATT&CK Navigator tool, it is possible to view all of these techniques at once in context of the entire ATT&CK Framework. The REvil-specific Techniques and Sub-techniques are highlighted in blue. An interactive, online version of this chart can be viewed directly on this page of the ATT&CK Navigator.

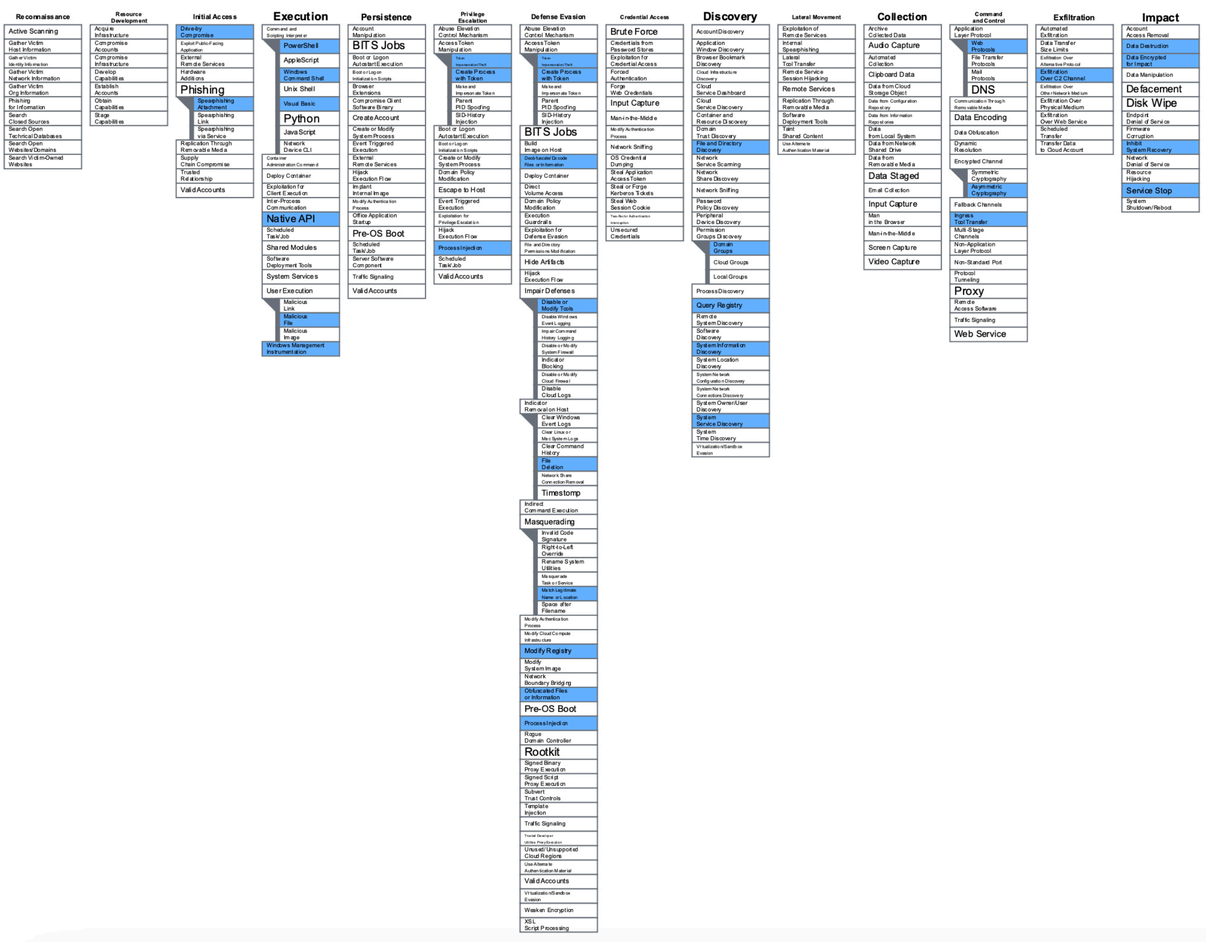


**FIGURE 6. ATT&CK NAVIGATOR VIEW OF REVIL'S TECHNIQUES**

The following outline provides a high-level view of the adversary's operation.

**Initial Access**

- T1189 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

## Initial Access

Initial access covers how an adversary gains access and establishes a foothold to a victim's environment. There are multiple ways that ransomware can make its way to a target's machine, but REvil operators prey on end users by spreading phishing emails or compromising legitimate sites to trick users. REvil was seen employing human-operated attack methods to target organizations that are most vulnerable to disruption. This would cover places that have limited time and resources to install latest patches or update firewall configurations, etc. This gives the adversary an advantage and insight for exploitation of these vulnerabilities in following phases of the attack (Waldman, 2020)

### T1189 Drive-by Compromise

Adversaries can gain access to a system or environment by having a victim access a legitimate website that is hosting hostile code that was planted by the adversary. Code injections, built-in interfaces, or malicious ads can be deployed on such compromised sites. The process often begins with a visitor connecting to a website that the adversary controls, after which malicious scripts will execute and drop ransomware variants.

REvil has been seen to infect victim machines through compromised websites and exploit kits. In one case, REvil was leveraged in a strategic web compromise by replacing WinRAR installation executable with an instance of the ransomware to infect the system. REvil has also been seen to compromise WordPress sites and inject JavaScript over the content of the original site in order to spread itself.

### T1566.001 Phishing: Spearphishing Attachment

One of the most common vectors for ransomware to get into environments is through targeted phishing attacks. These often are in the form of seemingly harmless emails that contain malicious links or attachments. REvil has often been distributed via malicious email attachments (e.g., Microsoft Word documents).

In addition to phishing attacks, reports released by both Group-IB (Group-IB, 2021) and Secureworks (Secureworks, 2019) show initial access can be obtained via Remote Desktop Protocol servers exposed to the public. In these cases, REvil operators would compromise the server using techniques such as Password Guessing [T1110.001] or Credential Stuffing [T1110.004]. After that, operators gained access via an external remote service and deployed ransomware. The report by Group-IB also notes that Virtual Private Network clients that do not utilize multi-factor authentication were another vector for initial access.

Another common entry point for initial access can occur when a threat actor is able to compromise a vulnerable application that is exposed to the public. (Group-IB, 2021)

## Discovery

Ransomware operators tend to use discovery techniques to supplement their attack plans for lateral movement and/or further collection on victims. Discovery techniques cover a wide range of activity, many of which are commonly shared across all types of malware.

### T1082 System Information Discovery

This technique encompasses a wide range of activity related to the host machine's system data. Types of system data include information about the operation system, versioning, patches, computer architecture, etc. Some ransomware has been seen evaluating the language of a system in order to determine whether the target is appropriate. The malware may also check whether the infected machine has language from the adversary's home country and/or may only wish to obtain ransoms from specific countries. Ransomware will look for this data in the beginning of the operation and may check the findings against a list and either have the ransomware exit or execute additional instructions based on its findings.

REvil looks for specific information about each host upon infection of a system. The general items that REvil is looking for are the machine name, operating system (OS) version, and the system language and keyboard layout information. REvil has been seen to ignore a set of languages (e.g., Arabic, Russian) and if a different system language is detected, it will continue on the normal flow of operations.

### T1083 File and Directory Discovery

This technique performed by REvil is performed by many different malware families, but it is particularly essential for ransomware due to its need to search for files of interest to encrypt as part of the locking process. Ransomware will often

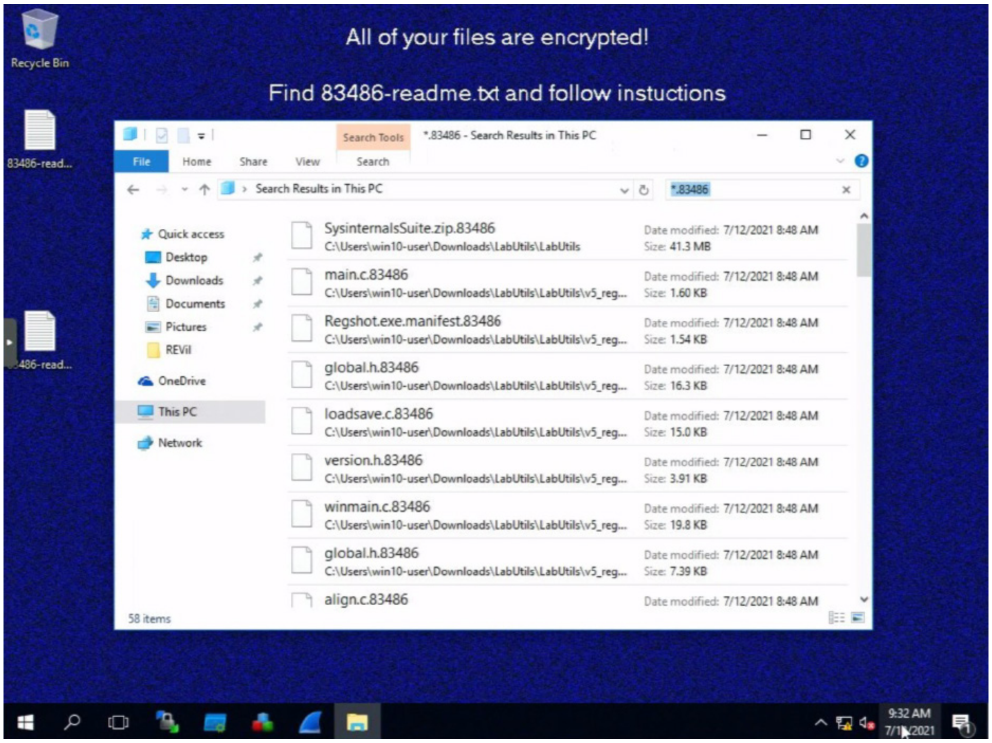


FIGURE 7. REVIL PERFORMING FILE SEARCHING ON THE SYSTEM

search for files of interest and determine what it will collect and encrypt from the victim. Once files are locked and encrypted, it is often too late, so prioritizing this type of behavior is imperative. For drive enumeration, some ransomware will use native application programming interface (API) calls such as GetLogicalDrives() for all mounted drives that have an Address Resolution Protocol entry and GetDriveTypeW() to determine the type of drive.

REvil has been seen to perform file discovery using several built-in commands and functions. In REvil's configuration, a field exists that enumerates which target extensions are to be avoided during encryption, as well as folders that should be encrypted. This selection process helps to ensure that critical files in the system are not destroyed. Before encryption begins, REvil will iterate through all folders and files residing on local fixed drives to verify that they are not in the configured list, as seen in **Figure 7**. If the file is deemed to not be included in the configuration, REvil will queue it and perform encryption afterwards.

### T1007 System Service Discovery

Services are another component that ransomware will often discover. Ransomware will enumerate the running services on a system using built-in commands or tools (e.g., tasklist, net start, etc.). The malware may attempt to disable or stop security services that hinder its progression in the locking process.

To find out what services are available, REvil will first enumerate active services on the system. This allows it to determine what services can be leveraged, as well as which services might need to be disabled. Service discovery may lead to the adversary choosing to use the techniques *Disable or Modify Tools* [T1562.001] or *Service Stop* [T1489].

### T1012 Query Registry

The Windows Registry contains a significant amount of useful information for adversaries, which is often inspected by ransomware.

REvil uses the Registry for multiple components of its attack. To prepare the files for encryption, REvil has been seen searching the Registry key Software\recfg for the presence of the rnd_ext value, and this randomly generated value will be appended to the files selected for encryption. (Counter Threat Research Team, 2019)

### T1069.002 Permission Groups Discovery: Domain Groups

Adversaries will search for domain-level groups and permission settings to help determine which groups exist and which users belong to a certain group. This can be used to determine which users have elevated permissions that can be targeted. Through this technique, REvil operators can identify the domain membership of a compromised host. It has a field in its configuration to look up the machine domain and workgroup.

## Defense Evasion

Another important part of the ransomware infection process is to avoid being detected by analysts. The malware uses many of the following behaviors to hide its activity. This is especially important for ransomware, as it needs to remain undetected while starting the encryption and locking of targeted files. If the ransomware is detected before the files can be encrypted, then its operation could be compromised. Defenders are strongly urged to prepare in advance and not depend upon identifying the malware before it starts the encryption process.

### T1036.005 Masquerading: Match Legitimate Name or Location

Ransomware has used a variety of masquerading techniques to evade detection. This usually consists of renaming malicious executables to names that are known to be benign. Other than renaming executables, the malware can also place such files in strategic locations, like trusted directories.

Many of REvil's artifacts mimic the names of known executables. This is done so REvil can avoid being detected. In one case, it changed the name of its executable file to "Microsoft-Word.exe" to pass as a benign and non-suspicious file. This is helpful to ransomware because it keeps activity hidden until the user notices or is suspicious of the file. Until it has been confirmed to be malicious, the ransomware can continue the infection process.

### T1562.001 Impair Defenses: Disable or Modify Tools

Adversaries using ransomware may attempt to disable active security tools or services so they can remain undetected through the infection process. This is particularly common with ransomware in order to lock files. Ransomware may also disable dynamic analysis tools, debuggers, and real-time monitoring features.

In REvil's case, it has demonstrated its ability to connect and disable the Symantec server on a victim's network. (BlackBerry Cylance Threat Research Team, 2019).

### T1070.004 Indicator Removal on Host: File Deletion

Ransomware has been seen deleting itself from a system as well as deleting any additional payloads or launchers after execution. Any scripts or log files might also be cleaned from the disk to further evade detection of the ransomware.

REvil has been observed marking its binary code for deletion during reboot. By deleting its code, operators can hide components of the attack and make it harder for analysts to explore the code of the ransomware, to detect or defend against it. Removal of files can occur before or after an intrusion and can be performed with a number of different tools (e.g., SDelete and DEL).

REvil set up its code for deletion after infection, which means it likely occurred during the post-exploitation phase. This functionality can often be built in to ransomware variants or executed via a command shell.

### T1027 Obfuscated Files or Information

This technique is commonly executed by all malware, including ransomware. Because of how common it is, it may not necessarily be indicative of ransomware behavior, but it is something that will likely occur with a ransomware attack. During the encryption process, ransomware might obfuscate strings and API functions to hide from detection. It may also pack samples to prevent analysis.

REvil has been observed using encryption to mask strings and configuration files to conceal as many of its components from analysts as it can. Its goal is to avoid getting caught and to make it harder for malware analysts to learn more about its behavior if it is caught.

### T1055 Process Injection

Ransomware can leverage this technique, much like other types of malware. It can inject reflectively into memory of legitimate running processes or load encrypted Dynamic-Link Libraries (DLLs) into new processes. Ransomware operators will do this to evade detection and elevation of privileges.

REvil operators have been seen using batch files to download payloads from Pastebin and then injecting them into a process on the operating system. This helps to hide the malicious process from detection and likely to elevate system privileges. (Saavedra-Morales, 2019).

### T1134.001 Access Token Manipulation: Token Impersonation/Theft

REvil can obtain the token from the user who launched the explorer.exe process to avoid affecting the desktop of the SYSTEM user.

### T1140 Deobfuscate/Decode Files or Information

Ransomware may decrypt its payloads, scripts, and other artifacts. Ransomware will often be obfuscated for these anti-analysis purposes, and these encoded items must be decoded once brought into the network.

REvil has been seen decoding encrypted strings to enable execution of commands and payloads. Artifacts from a ransomware intrusion are hidden from analysis using a variety of obfuscation techniques that eventually need to be decrypted by the operators.

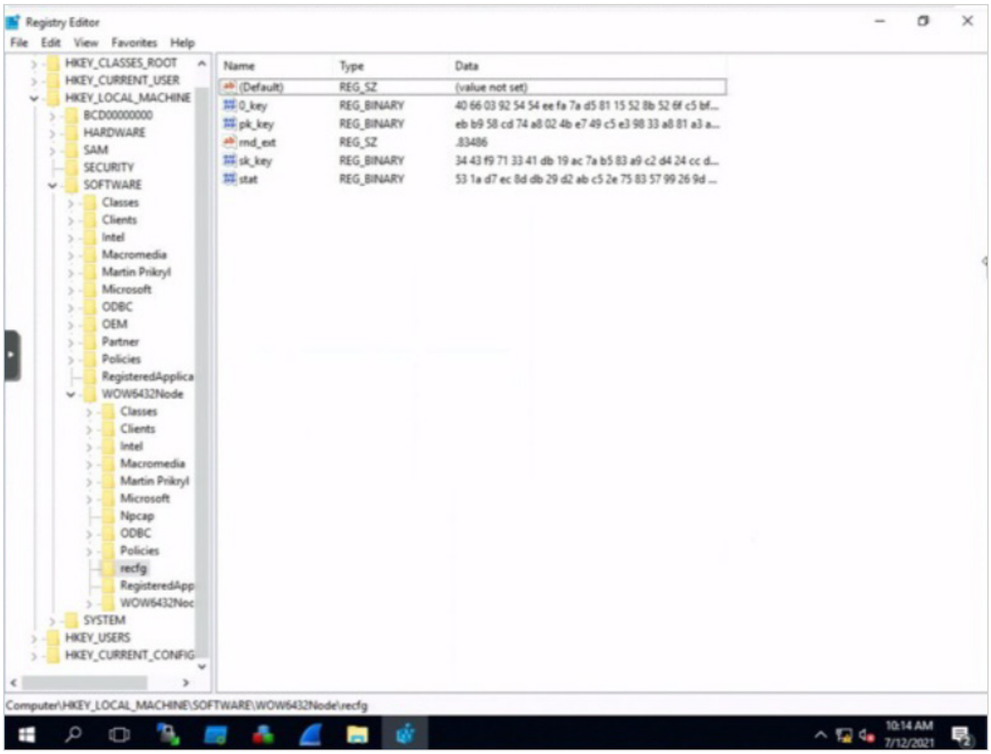


**FIGURE 8. REGISTRY MODIFICATIONS MADE BY REVIL IN THE MITRE LAB**

### T1112 Modify Registry

Ransomware will use the Registry to help store components needed for the encryption and decryption process. This often consists of the different keys needed, based on the encryption method. Many ransomware authors will also modify the Registry to store victim information. Modification of the Registry can help reduce footprint and provide cleanup of artifacts, but it can also aid in persistence in execution phases of the attack.

REvil can save encryption key parameters and system information to the Registry. See **Figure 8** for how that may look on a system. During execution, REvil has been seen to write in the Windows Registry entries under the subkey "SOFTWARE\recfg." The Registry key entries that are added have been for the master key, which is used for encryption later; the victim's private key, which is used for file decryption; information gathered from the victim's machine; and a random extension for the encrypted files. In **Figure 8**, REvil has made modifications to the Registry.

## Privilege Escalation

These techniques occur when the adversary is looking to gain high-level permissions (e.g., SYSTEM/root, local Administrator, user account with Administrator access, etc.).

### T1068 Exploitation for Privilege Escalation

Ransomware operators will try to exploit software vulnerabilities to elevate privileges to perform additional tasks on a victim's machine. The REvil ransomware has a built-in flag that can be set when it wants to attempt to run with elevated privileges. To gain SYSTEM privileges on the infected host, it will try to exploit the kernel-level vulnerability in win32k.sys, which is known as CVE-2018-8453. Exploiting these vulnerabilities will help to bring privileges to a higher level so that more sophisticated tasks can be performed on the victim's machine.

### T1134.002 Access Token Manipulation: Create Process with Token

Ransomware and other malware will create a new process under the security context of a different user to increase privileges. REvil can launch an instance of itself with administrative rights using the run as command to elevate privileges.

## Execution

Ransomware may use a remote access tools or Windows Management Instrumentation (WMI) to run PowerShell or Visual Basic Script (VBS) scripts that can perform additional tasks to supplement the ransomware objectives.

### T1047 Windows Management Instrumentation

WMI can be leveraged to perform several operations that are specific to ransomware. Leveraging this tool in conjunction with ATT&CK techniques that fall under the Impact tactic will be one way to determine whether ransomware is infecting a system. WMI can be used to interact with local and remote systems as well.

REvil has leveraged *Windows Management Instrumentation (WMI)* [T1047] to continuously monitor for and kill newly launched processes whose names are listed in the configuration key. REvil has also been observed using the *PowerShell* [T1059.001] command "Get-WmiObject Win32Shadowcopy | ForEach-Object {$_.Delete();}" to delete shadow copies. (Intel 471, 2020)

### T1059.001 PowerShell

PowerShell is a powerful tool used by many adversaries and many different types of malware. Ransomware is no exception, as it has been observed using this method to execute parts of the infection process, as well as to perform tasks with stealth. This method has been used by operators to deploy ransomware and to write code to avoid detection. Ransomware has also been seen to use *PowerShell* [T1059.001] scripting as a means to decode or decrypt obfuscation letters and to use encoded PowerShell commands to create services.

REvil operators have specifically been seen using PowerShell to delete volume shadow copies and download files to the victim's machine. While these tasks are distinct ATT&CK techniques, the use of PowerShell to achieve them is worth recognizing because it is a Microsoft scripting language whose use can be mistaken for legitimate activity.

### T1059.003 Windows Command Shell

Ransomware uses the Windows command prompt, usually to achieve task execution. Batch files also provide the shell with a list of sequential commands to run; many ransomwares will use these batch scripts to execute several components of the attack.

REvil has used the Windows command line to delete volume shadow copies and disable recovery. Deleting these items is covered in another technique, but this technique is important to recognize since it is a means of achieving other tactical goals, like Impact and Defense Evasion, since the command shell is needed to execute components of these tactics' attacks.

### T1059.005 Visual Basic

Malware and ransomware often use a variety of scripting tools to execute specific tasks on a victim's machine. In the case of REvil, it can split Visual Basic for Applications (VBA) codes into modules and functions embedded within Word document macros to conceal its activity and to execute tasks on the system. Scripting in all varieties will usually be supplemental to the objectives of the ransomware, and it will aid in the infection process by helping to complete tasks that can be automated, so the adversary can focus on more sophisticated components of the attack. VBA scripts can help ransomware identify victim information and distribute additional malicious files to the system. In REvil's case, it is used obfuscated VBS scripts to perform execution.

### T1106 Native API

Ransomware will use this technique to interact directly with the operating system and carry out tasks and requests during routine operations. In addition to execution, the built-in API can be used to add a layer of protection to evade detection and leverage functions to inject ransomware.

REvil has used built-in API functions to perform execution and to retrieve active services. REvil has been seen doing this during its initialization period. The malware dynamically resolves the library imports it needs and then reads them to the appropriate API function. After this, the malware can execute additional code needed for the ransomware infection process.

### T1204.002 User Execution: Malicious File

This technique frequently occurs shortly after Initial Access. Adversaries that are deploying ransomware will rely on a user to open a malicious file in order to execute something. In most cases, ransomware has been seen to use malicious files in the same way that traditional malware does, which is to lure victims into clicking and unknowingly executing the code so the infection process can begin.

REvil has been executed via malicious Microsoft Word email attachments. These files are sent via *Spearphishing Attachment* [T1566.001], but then are dependent on the user clicking on the malicious file in the email in order to get REvil executed on victim's machine. Once that malicious file has executed REvil, the rest of the infection process can begin. In one instance, REvil operators sent a malicious document that asked the victim to enable content, and when the victim clicked enable, the hidden code in the macros launched REvil ransomware.

## Command and Control

Adversaries will set up a C2 channel to help communicate with compromised systems. Ransomware will likely need to have a communications channel to ensure files are encrypted and to exfiltrate files and folders for double extortion ransom.

### T1071.001 Web Protocols

This is a commonly shared technique among all types of malware, including ransomware. Ransomware operators need a communication mechanism to communicate with their malware and/or extract data from the victim's system. Candidates for this communication include common web protocols like HTTP or HTTPS, which is commonly allowed access to the internet. This allows the adversary to blend in with existing traffic more easily. REvil has been seen using both HTTP and HTTPS for communication with its C2 server.

### T1105 Ingress Tool Transfer

This technique is used by many adversaries and shared among ransomware and other malware. Ransomware tends to leverage it in the same way traditional malware does. Files are downloaded and uploaded to a system for further execution or as a means of C2. Ransomware operators usually depend on a set of tools that can allow them to perform different actions during the post-exploitation phase, and sometimes these utilities are not in the victim's environment, so they will need a method to bring in tooling from an external resource.

REvil operators have been seen using the URLDownloadToFile function to bring temporary files onto the system to aid in executing the REvil ransomware file. Operators have also been seen using *PowerShell* [T1059.001], *Windows Command Shell* [T1059.003], and the Certutil utility to download these additional files.

### T1573.002 Asymmetric Cryptography

Asymmetric encryption can help adversaries conceal C2 traffic rather than depending on inherent protections provided by a standard communication protocol. This ensures that the ransomware operators' communications with the victim's machine are concealed and more difficult to detect.

REvil has encrypted C2 communications with the ECIES algorithm and AES-256-CTR. (Orkhan, 2019)(Counter Threat Research Team, 2019). It uses a symmetric algorithm in conjunction with an asymmetric key exchange method. Since it uses an asymmetric key scheduling algorithm, it does not depend on network communication to exchange encryption keys with the REvil operators.

## Exfiltration

Exfiltration occurs in ransomware for many reasons. As the ransomware is infecting a system, it may attempt to send back basic information gathered about the host to determine whether it is appropriate for encryption. The ransomware would also likely send back files of interest, especially if it will be selling the data or extorting money from the victims. The ransomware operator can post exfiltrated data publicly or auction it off.

### T1041 Exfiltration Over C2 Channel

Ransomware will exfiltrate data over the C2 channel to extort the victim by threatening to publish the stolen data. The C2 channel is where the adversaries are waiting to receive information about victims, and the channel is used for taking data out of the victim's system and bringing it to the adversary's environment.

REvil has been seen to have the functionality to collect and exfiltrate basic host and malware information and send it over the configured C2 server. This is a task that helps with learning more about the victim's environment and/or extracting information for other purposes. Since REvil takes out data via exfiltration, it has been used to set up auction pages that sell the victim's sensitive data to the highest bidder.

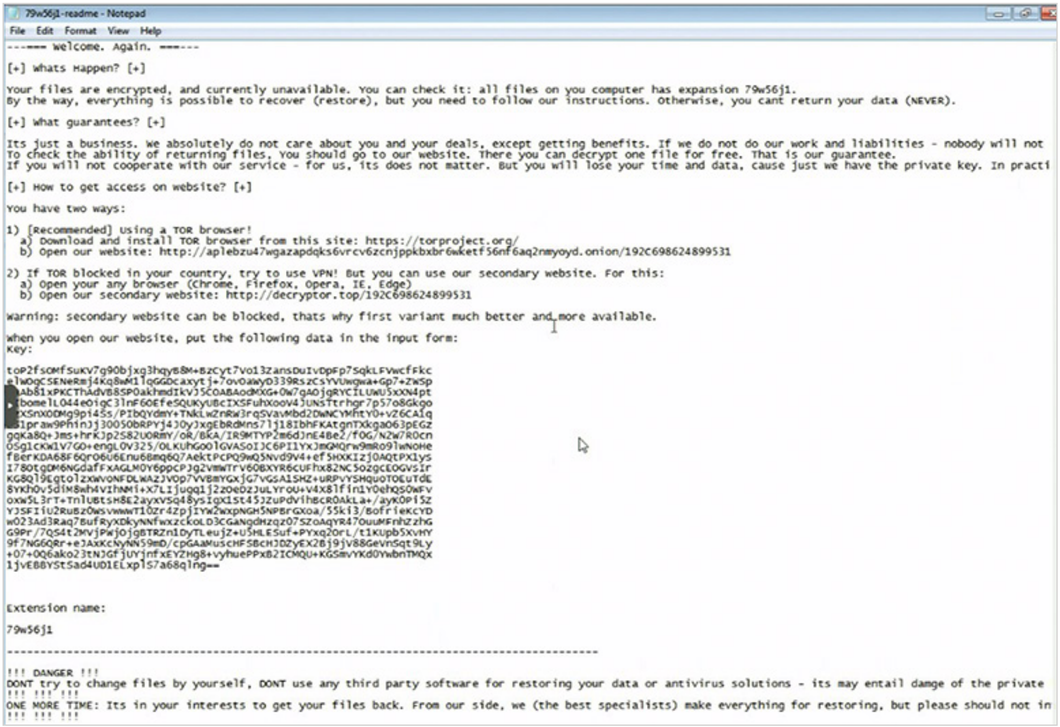


**FIGURE 9. RANSOM NOTE DROPPED BY REVIL TO VICTIM'S MACHINE THAT DETAILS HOW TO PAY THE RANSOM**

## Impact

Adversaries will achieve impact by trying to manipulate, interrupt, or destroy systems and data. In the case of ransomware, this can help set it apart from other malware. This tactic was created to capture ransomware activity and to include different attack vectors from traditional malware. When the ransom is not paid, ransomware can become destructive.

Some of these capabilities can be set up before the encryption begins but executed afterwards if the ransom is not met.

Ransom notes may be left on systems once the files have been locked and the attacker is ready to ask the victim for money. REvil's ransom note includes information on what is happening, what is guaranteed, how to regain access to files, and where to pay the ransom to obtain the decryption key. These are all pretty standard outlines for how ransom notes go, and by the time this phase is achieved, the attacker has already impacted the affected organization and bypassed any mitigations that may have been in place.

### T1489 Service Stop

This technique involves the stopping of critical services (e.g., anti-virus, backups, security-related, database, email solutions, etc.). Ransomware operators may use "net stop" to accomplish this. Ransomware also has killed processes and/or services associated with Exchange, Microsoft Structured Query Language servers to make it possible for them to encrypt those data stores. Other types of business applications and databases that contain files of interest might have their services targeted and terminated for file encryption.

Stopping Services has also been observed by REvil, in which it will call a batch script, kill.bat, to disable services and processes prior to encryption. This happens earlier on to aid in the damage or adversary's objectives to cause damage to the environment. By disabling security services or processes, REvil can bypass controls that would have prevented specific techniques it needs to accomplish file encryption. REvil also has a field in its configuration to list out the processes that need to be terminated for unlocking files that are locked by these programs (e.g., mysql.exe). These get terminated if they are found on the system.

### T1490 Inhibit System Recovery

Adversaries may delete or disable system recovery features to increase the impact of other ransomware techniques. Often, ransomware will delete the system's shadow volumes to prevent recovery. This can occur more than once, with the first instance being before the encryption process and the second being after. Tools that can be used to perform this are vssadmin, wbadmin, bcdedit, wmic, and others. This behavior augments the effects of *Data Destruction* [T1485] and *Data Encrypted for Impact* [T1486] techniques.

REvil uses vssadmin to delete volume shadow copies. This makes it so users cannot recover or repair lost files since it deletes the recovery copies that would have been stored on this system. Ransomware will do this to avoid having the victim recover their files without paying the ransom.

### T1486 Data Encrypted for Impact

What differentiates ransomware from other malware is the intent to encrypt system data to extort money from the victim in exchange for a decryption key. When determining if the malware that has made it into the environment is ransomware, looking for behaviors surrounding file encryption is key. Individual files are destroyed or overwritten so the data cannot be recovered, which increases the impact of locking files for ransom. The higher the impact of the locked files, the higher the chance the victim will be influenced into paying the ransom so they can recover their files.

After REvil has set the scene and determined which files and folders will need to be encrypted, it can begin that process. The process usually begins with reading the file into a buffer, then encrypting the contents of that buffer. The encrypted contents of the buffer get written to the original file, which overwrites the original content. Then REvil will rename the original file with a randomly generated extension. File contents have been encrypted by REvil with the Salsa20 symmetric stream algorithm. REvil uses an extremely fast encryption method and multi-threading to fully consume the host's available resources. The only way victims will be able to decrypt the encrypted files is to obtain the private key from REvil operators.

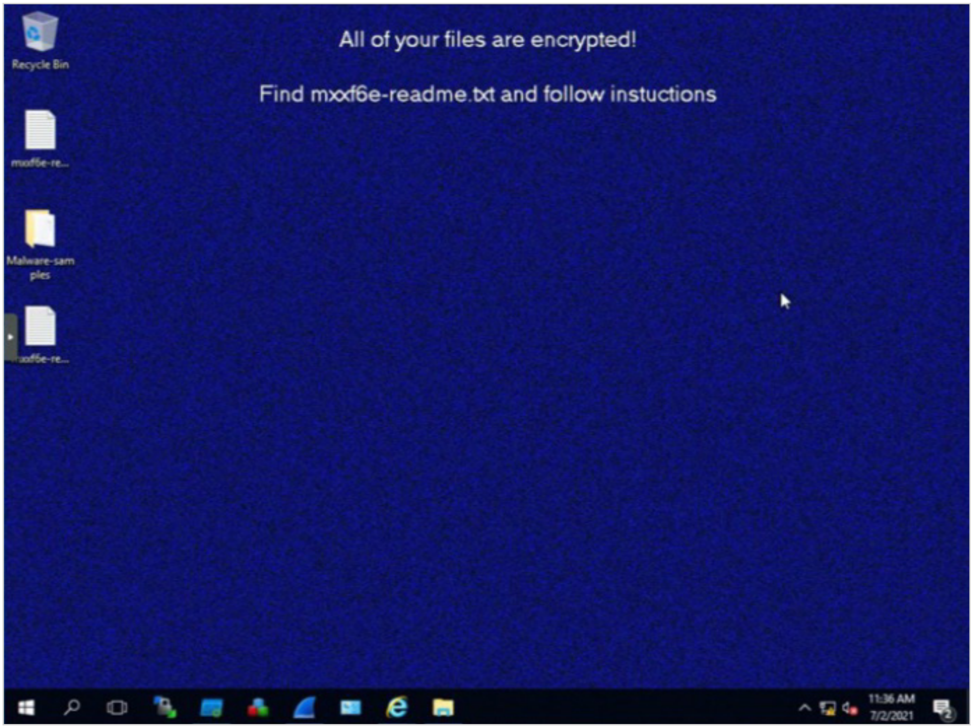


FIGURE 10. REVIL HAS ENCRYPTED THE SYSTEM FILES AND CHANGED THE DESKTOP WALLPAPER TO NOTIFY AND INTIMIDATE THE USER

### T1491.001 Defacement: Internal Defacement

Ransomware will often deface internal systems, attempting to intimidate users. This takes the form of websites and/or replacing the desktop wallpaper to cause the user discomfort and pressure them to pay associated ransoms.

REvil will change the background desktop wallpaper to be set with the ransom note, as seen below in **Figure 10**. REvil can generate a bitmap image and set it as the desktop background, explaining that files have been encrypted and instructing users where to find follow-up information.

### T1486 Data Destruction

If the victim refuses to pay the ransom, adversaries, like the ones using REvil, may threaten to destroy and wipe the data on the system. This can be highly motivating for organizations that lack offline backups or alternative operating processes, especially if the data in question is difficult to replicate. The process of destroying data usually leaves it irrecoverable because the ransomware will override files and data on drives. This increases the overall impact of locking the files for ransom.

REvil has been seen searching the local fixed drives and network share for folder names that match the list of names it has, and then it will erase the file contents of blacklisted folder and subfolders, but will not delete them. REvil will only wipe the contents of folders named "backup" but will skip other ones. The built-in wipe function, which has been seen in REvil's configuration data, will destroy the target files that have a specific field value called "wfld." This destruction will occur in all folders that match that name and can be overwritten with trash data or null data, depending on the sample variant.

## Ransomware Mitigations and Detections

By the time an organization receives a ransom letter, it is too late to stop the attack. The focus of defenders should be to prepare for the attack in advance by, at a minimum, performing backups of all critical data and preparing alternative means to operate. After backups and alternative operations have been planned, implemented, and tested, the next step organizations can take to minimize the attack surface is to perform cyber hygiene best practices such as patching, hardening, isolating high-risk environments, and implementing least privileges. The final step would be to implement sensors and analytics to detect ransomware after it has breached an organization's defenses, but before it has encrypted the data or rendered computers inoperative.

This section will only look at the means to implement analytics that respond directly to REvil, as a case study. For details on how an organization should prepare in advance for a ransomware attack, please see additional resources here.

In some cases, a narrow window of opportunity exists after initial penetration, while the ransomware is still actively discovering the environment, moving laterally from system to system, downloading tools, and preparing to encrypt the data. Organizations should not depend upon attempting to detect ransomware after it has breached a computer network as their primary defense. This effort should be considered the final defensive measure in a defense-in-depth strategy, a means of last resort to try to be aware of the ransomware breach before the encryption and subsequent ransom letter.

To achieve detection, organizations should increase their visibility of the network and on endpoints, watching for suspicious behavior to provide early warning signs before the encryption occurs. Instrumenting endpoints with increased data collection and analytics to identify these behaviors is likely the best means to achieve such detection. This section will outline approaches for doing so.

It should be noted that detections and mitigations can be evaded. No defensive measure is foolproof, which is one of the reasons for a defense-in-depth strategy.

### Analytics Strategy

A security team implementing analytics will need to prioritize which behaviors they will attempt to detect. The security team should focus on those behaviors that can be easily distinguished as malicious, rather than benign. For specific ransomware or malware, individual TTPs can be broken out, and specific procedures can then be reviewed and used to help make more impactful detections that will be beneficial for avoiding compromise. However, this is simply a way to prioritize TTPs; as resources permit, other TTPs should also be examined. Filtering on specific adversary groups and ransomware variants that target a specific industry may be useful, as it is unlikely that an organization will only be targeted by adversaries or ransomware that is publicly documented. It is important to recognize that adversaries often adapt with new TTPs and may attempt to change the way they perform types of attacks so they can escape detection. Breaking out all of the techniques in this way can be exhausting, so it would be better to determine which adversaries and ransomware variants are most likely to target the organization and then compare those layers in the ATT&CK Navigator to choose the TTPs to explore.

## Defensive Strategy

### General Preparation

Being prepared for a ransomware attack is of paramount importance. Having established procedures in place prior to an attack will enable an organization to respond to a ransomware incident more effectively.

Organizations must conduct regular vulnerability assessments and threat modeling to uncover potential vulnerabilities in the organization's attack surface, and identify areas where necessary process and procedures may be missing or outdated.

An organization's risk assessment will also identify systems that would be high-priority target for a ransomware attack because they contain sensitive information. Organizations should create a plan to ensure that these high-value targets are hardened, patched regularly, and that access to these systems follows the principles of least privilege.

Lastly, the analytics gathered by an organizations security team should be used to establish baselines for key workflows and expected behaviors for systems that contain sensitive data. Having this information documented can assist an organization in the creation of activity monitors that can then be used to alert on the early stages of a ransomware attack. These activity monitors can also be implemented to help with early detection.

### Incident Response Process Preparation

Establishing an incident response plan specific to ransomware attacks can lead to a more predictable outcome for an organization. Organizations should have a plan for some sort of dedicated incident response team, whether that is in-house or contracted out. Establishing a primary and secondary incident commanders within the organization can be beneficial in many ways. The primary responsibilities of incident commanders are to coordinate and assist subject matter experts (SMEs) with responding to and mitigating an incident. Many hospitals already have an incident command system that can be utilized for cyber response, and preparing that team can be vital for managing the response to a ransomware attack.

Having an established incident response plan in place and understanding what triggers the declaration of an incident will provide focus to the response team and eliminate guesswork during a stressful situation.

The incident response needs to be practiced on a regular basis (at least bi-annually) so that incident commanders and SMEs are familiar with the process, rather than having to adapt under the less-than-ideal circumstances of an actual incident. This will have the added benefit of ensuring that other aspects of the response, such as the quality of backups and the disaster recovery process, are tested on a regular basis.

### Incident Recovery

Organizations must have an established disaster recovery plan in place, and it should be linked to the incident response plan for a ransomware attack.

Recovering from a ransomware attack will rely on an organization's overall data backup process. As part of general preparation, ensure that the systems the organization relies on for recovery have been hardened and isolated from the corporate network.

Make sure that the organization's incident commanders and SMEs understand the disaster recovery plan, and when it is appropriate to initiate it.

Organizations should make sure that both the incident response and disaster recovery teams participate when it comes time to practice the overall response to a ransomware attack.

### Recommendations for Smaller Organizations

For organizations that have limited security resources or lack SMEs within their organization to assist in responding to a ransomware attack, the following recommendations can assist in establishing a baseline defense.

Establish a security training program that covers baseline best practices and specific training and awareness that covers phishing and other initial access vectors.

Members of the organization who have access to sensitive data should receive additional training on the responsibilities associated with accessing sensitive data. The organization's security training program should be conducted annually.

If the organization is unable to conduct its own threat assessment, then consider hiring a reputable third-party penetration testing company to assess the organization's overall security posture. The resulting report helps organizations understand where they are vulnerable and where they should prioritize putting process and mitigations in place.

"How will our organization respond to a ransomware attack?" Answering this question can be used to create a playbook. This playbook should cover the organization's initial response to the attack and how they plan to recover. Once the playbook is in place, it should be practiced on a frequent basis (quarterly).

## Responses to Specific Techniques

This section outlines detections and mitigations for each of the REvil Techniques and Sub-techniques that have been observed and reported by public CTI and as outlined above in Section 3, Detailed REvil Tactics, Techniques, and Procedures. The Techniques and Sub-techniques are organized by Tactic.

### Initial Access

#### T1189 Drive-by Compromise

**Threat Detection**

Implement least privilege firewall policies and inspect URLs for known malicious domains or parameters. Reputation-based analytics may also be available to evaluate parameters such as the age of a domain, the party it is registered to, and how many users have connected to it in the past. Network intrusion detection systems might help identify malicious scripts and obfuscation code.

| Analytic ID | OS | URL | Source Repository |
| --- | --- | --- | --- |
| eb07e747-2552-44cd-af36-b659ae0958e4 080bc66a-5d56-4d1f-8071-817671716db9 | Windows | https://github.com/SigmaHQ/sigma/blob/1ff5e226ad8bed34916c16ccc77ba281ca3203ae/rules/windows/dns_query/sysmon_possible_dns_rebinding.yml | Sigma |
| 080bc66a-5d56-4d1f-8071-817671716db9 | Mac | https://github.com/elastic/detection-rules/lblob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/macos/execution_initial_access_suspicious_browser_childproc.toml | Elastic |

**Mitigation**

Software should be patched and kept current. Wherever possible, modern browsers and plug-ins should be used. Restrict web-based content (e.g., ads, ad blockers) to prevent untrusted code from executing on an organization's systems. Additionally, script blocking extensions can help protect against JavaScript injections. Virtualization and browser sandboxes can provide additional mitigation. Control flow integrity can potentially block software exploitation, and security applications can be implemented to mitigate exploitation behavior. If possible, implement whitelisting of applications.

| Mitigation ID | Name | Description |
| --- | --- | --- |
| M1021 | Restrict Web-Based Content | As mentioned above, malicious code can be delivered in several ways via a browser. Installing ad blockers on all endpoints within an organization will help prevent the execution of malicious code. Security teams can also deploy a Domain Name System (DNS) sinkhole that is configured to drop outgoing requests to known malicious ad sites. |
| M1051 | Update Software | The web browsers used on all endpoints must be kept up-to-date. Most modern browsers will alert a user when updates are available. Organizations must have a process in place that defines how often software is be updated, and this must be communicated to users when joining the organization and re-enforced during annual security training. |

## T1566.001 Phishing: Spearphishing Attachment

### Threat Detection

Educate users on recognizing phishing attacks, and require annual security training for being informed.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 295a59c1-7b79-4b47-a930-df12c15fc9c2 | Windows | https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/registry_event/sysmon_registry_trust_record_modification.yml | Sigma |
| a624863f-a70d-417f-a7d2-7a404638d47f | Windows | https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/initial_access_suspicious_ms_office_child_process.toml | Elastic |

### Mitigation

User training can help employees and staff understand social engineering techniques and not be tricked by them. Restrict web-based content so that unknown or suspicious attachments are not transmitted by default over email; email scanning devices can also help analyze them. Using anti-spoofing and email authentication mechanisms to filter messages based on validity checks can enable recipients to perform messaging filtering and validation. Anti-virus and network intrusion prevention systems can further quarantine and prevent or block malicious email attachments.

| Mitigation ID | Name | Description |
|---|---|---|
| M1049 | Anti-virus/ Antimalware | Running anti-virus scanners on all client endpoints that look for known REvil signatures can help prevent the initial access of a ransomware attack. Regarding Windows endpoints, ensure that Windows Defender is enabled, as this will provide additional protections against malware. |
| M1017 | User Training | Establishing a baseline security training program within an organization for all users will educate them on basic security practices and inform them not to download and execute email attachments. |
| M1021 | Restrict Web-Based Content | The REvil samples that MITRE's team tested in the lab were Windows executables (.exe) files. Putting a policy in place to block transmission of .exe files and regularly scanning files attached to incoming corporate emails will help to prevent REvil from getting into an organization's environment. |

## Discovery

Discovery behavior can be difficult to detect, since it can often be confused with regular user activity. To distinguish malicious vs. benign activity, it is essential to capture the full command line as well as the parent process.

When an adversary first enters the host, they will try to determine some basic information such as software configurations, network environment information, and user data. The CAR-2016-03-001: Host Discovery Commands analytic can provide a good starting point for detecting this behavior. The CAR-2013-04-002: Quick execution of a series of suspicious commands analytic can provide a foundation of basic detections for a variety of other Discovery and other tactics' techniques. The coverage is considered low on these because a more sophisticated adversary can attempt to work around them, but they are somewhere to start when looking at user behavior.

### T1007 System Service Discovery

**Threat Detection**

Monitor processes and command-line arguments for actions that can be taken to gather information related to services. Tools such as PowerShell and WMI can be used to acquire this information.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 970007b7-ce32-49d0-a4a4-fbef016950bd | Windows | https://github.com/SigmaHQ/sigma/blob/ff0f1a0222b5100120ae3e43df18593f904c69c0/rules/windows/process_creation/win_query_registry.yml | Sigma |
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2013-04-002.yaml | CAR |

**Mitigations**

The technique above cannot be easily mitigated, because it is a system feature.

### T1012 Query Registry

**Threat Detection**

Monitor for interactions with the Windows Registry either through command-line utilities (e.g., Reg) or through the Windows API. WMI and PowerShell might also be used to grab information from the Registry, so examine these places too.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 970007b7-ce32-49d0-a4a4-fbef016950bd | Windows | https://github.com/SigmaHQ/sigma/blob/ff0f1a0222b5100120ae3e43df18593f904c69c0/rules/windows/process_creation/win_query_registry.yml | Sigma |
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2013-04-002.yaml | CAR |
| CAR-2013-03-001 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2013-03-001.yaml | CAR |

**Mitigation**

The technique above cannot be easily mitigated, because it is a system feature.

### T1069.002 Permission Groups Discovery: Domain Groups

**Threat Detection**

Monitor processes and command-line arguments for actions that can be taken to gather system and network information. WMI and PowerShell might be used along with remote access tools to acquire this information.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 75df3b17-8bcc-4565-b89b-c9898acef911 | Windows | https://github.com/SigmaHQ/sigma/blob/30bee7204cc1b98a47635ed8e52f44fdf776c602/rules/windows/process_creation/win_susp_adfind.yml | Sigma |
| eda499b8-a073-4e35-9733-22ec71f57f3a | Windows | https://github.com/elastic/detection-rules/blob/6ef5c53b0c15e344f0f2d1649941391aea6fa253/rules/windows/discovery_adfind_command_activity.toml | Elastic |
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-04-002.yaml | CAR |
| CAR-2016-03-001 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2016-03-001.yaml | CAR |
| CAR-2020-11-006 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2020-11-006.yaml | CAR |

**Mitigations**

The technique above cannot be easily mitigated, because it is a system feature.

## T1082 System Information Discovery

**Threat Detection**

Monitor processes and command-line arguments for actions that can be taken to gather system and network information. Information can be acquired via the Windows API, PowerShell, WMI, and other tools.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 2887e914-ce96-435f-8105-593937e90757 | Windows | https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_commands_recon_activity.yml | Sigma |
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-04-002.yaml | CAR |
| CAR-2016-03-001 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2016-03-001.yaml | CAR |

**Mitigations**

This technique cannot be easily mitigated, because it is an abuse of system features.

## T1083 File and Directory Discovery

**Threat Detection**

Detection of this type of activity is difficult since normal users often search their own system for files as part of routine behavior. It can be examined as part of a chain of activities to correlate the behavior as malicious. Detection of file and directory enumeration can begin with process monitoring for specific commands that have been used to gather files. Looking at whether remote access tools or built-in API functions are leveraged to gather information like this can help. File and directory enumeration may look different from a ransomware viewpoint.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 7b08314d-47a0-4b71-ae4e-16544176924f | Windows | https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/discovery_file_dir_discovery.toml | Elastic |

**Mitigations**

The technique above cannot be easily mitigated, because it is a system feature.

## Defense Evasion

### T1036.005 Masquerading: Match Legitimate Name or Location

**Threat Detection**

File monitoring and file hashing can be helpful for detection of this behavior. Look for files that are known names but located in unusual locations or modified outside of an update. File names should match the binary's Portable Executable (PE) metadata. Collection and comparison of disk and resources filenames for binaries can help bring about productive searches. For specific detection, look for command-line arguments that are known to be used.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2021-04-001 | Windows | https://github.com/mitre-attack/car/blob/b232cbdba0ce83870811bfeb88e934c4eaf04aa6/analytics/CAR-2021-04-001.yaml | CAR |

**Mitigations**

Require signed binaries and images, and use tools that restrict program execution via application control attributes other than file name. Restrict file and directory permissions by implementing file system access control to protect folders like C:\Windows\System32.

| Mitigation ID | Name | Description |
|---|---|---|
| M10838 | Execution Prevention | Within the organization, deploy tools that limit program execution on each endpoint. Limiting program execution via application control policies or using tools that allow for the creation of application whitelists will provide an additional layer of protection against the unintended execution of ransomware. |
| M1045 | Code Signing | Only permit the execution of signed binaries and images that come from trusted sources on endpoints within the organization. |
| M1022 | Restrict File and Directory permissions | All endpoints within the organization should have access controls in place to protect important directories such as C:\Windows\System32. |

## T1562.001 Impair Defenses: Disable or Modify Tools

**Threat Detection**

Monitor processes and ensure that security tools are running. The Registry can also monitor changes made to critical services and/or startup programs.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2016-04-003 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2016-04-003.yaml | CAR |
| CAR-2021-01-007 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2021-01-007.yaml | CAR |
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2013-04-002.yaml | CAR |

**Mitigations**

Several mitigations exist for this activity. Restricting file/directory and Registry permissions will help prevent adversaries from interfering with security services that can be modified. Ensuring that proper user permissions are in place based on users' needs to prevent adversaries from disabling or interfering with security services will also be critical.

| Mitigation ID | Name | Description |
|---|---|---|
| M1022 | Restrict File and Directory Permissions | Ensuring that process and file permissions are in place will help to prevent ransomware variants from disabling or interfering with security services. |
| M1024 | Restrict Registry Permissions | Some samples of REvil that were run in MITRE's lab made modifications to the Windows endpoint. To better protect endpoints within an organization, ensure that Registry permissions are in place to help prevent REvil ransomware from having an additional method of disabling or interfering with security services. |
| M1018 | User Account Management | Ensure that user permissions are set properly on all endpoints within an organization. REvil will look for ways to elevate its privileges, and having proper user permissions in place can assist in preventing REvil from disabling or interfering with security services. |

## T1070.004 Indicator Removal on Host: File Deletion

**Threat Detection**

Monitoring for command-line detection functions to correlate with binaries or other files may help identify malicious activity. Monitoring for known deletion, and secure deletion tools that are not already installed on systems that an attacker can use.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 6ddab845-b1b8-49c2-bbf7-1a11967f64bc | Windows | https://github.com/SigmaHQ/sigma/blob/1ff5e226ad8bed34916c16ccc77ba281ca3203ae/rules/windows/file_delete/sysmon_sysinternals_sdelete_file_deletion.yml | Sigma |

**Mitigations**

The techniques above cannot be easily mitigated because it is an abuse of a system feature.

## T1027 Obfuscated Files or Information

**Threat Detection**

Ransomware will seek to delete traces or artifacts left behind from the attack, so detection may be difficult or not possible. Since ransomware may try to obfuscate payloads, using network intrusion detection systems there can help. Flagging and analyzing commands that have known suspicious syntax like "^" or """ and Windows and Sysmon Event ID 4688 can help show command-line arguments.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2021-05-009 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2021-05-009.yaml | CAR |

**Mitigations**

Anti-virus solutions can help analyze commands after being processed.

| Mitigation ID | Name | Description |
|---|---|---|
| M1049 | Anti-virus/Antimalware | Windows 10 offers an Antimalware Scan Interface (AMSI) that integrates with User Account Control, PowerShell, wscript.exe, cscript.exe, JavaScript, VBScript, and Office VBA macros. An organization can use AMSI where appropriate to analyze commands as they are being processed to detect suspicious behavior. |

### T1055 Process Injection

**Threat Detection**

Specific Windows API calls are affiliated with modifying memory within another process, such as VirtualAllocEx()/WriteProcessMemory() and other process-related calls like CreateRemoteThread(), SuspendThread/SetThreadContext/ResumeThread(), and QueueUserAPC/NtQueueApcThread(). For DLL injections, monitor DLL/PE file events, specifically creation of these binaries and loading into processes. Named pipe creations and connected events (which fall under Windows Event IDs 17 and 18) can also indicate infected processes. Processes should have a baseline behavior to determine if/when they are performing unusual behavior (e.g., opening network connections, reading files, etc.).

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2020-11-004 | Windows | https://github.com/mitre-attack/car/blob/17fca00ded9fe006314c4651c94dedc885e04a74/analytics/CAR-2020-11-004.yaml | CAR |
| CAR-2020-11-003 | Windows | https://github.com/mitre-attack/car/blob/17fca00ded9fe006314c4651c94dedc885e04a74/analytics/CAR-2020-11-003.yaml | CAR |
| CAR-2013-10-002 | Windows | https://github.com/mitre-attack/car/blob/17fca00ded9fe006314c4651c94dedc885e04a74/analytics/CAR-2013-10-002.yaml | CAR |

### T1140 Deobfuscate/Decode Files or Information

**Threat Detection**

Monitor execution file paths and command-line arguments for common archive file applications and extensions. If scripts are used, then collection of scripts for analysis can help, and process and command-line monitoring can help detect utilities like certutil.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2021-05-009 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2021-05-009.yaml | CAR |

**Mitigations**

The technique above cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

### T1112 Modify Registry

**Threat Detection**

One place to start is to enable Registry auditing on specific keys to produce an alert (Windows Event ID 4657) when a value gets modified. Changes can also occur around new services and modification of binary paths that may point to ransomware in the startup locations. Monitor processes, command-line arguments, and API calls for actions around a user attempting to change or delete information from the Registry or using Reghide to conceal Registry keys. REvil has been observed to place configurations and encryption keys in the "Software\recfg" Registry subkey. The presence of this subkey can signify that REvil has infected the system, so monitoring around this subkey can help with detection.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2014-11-005 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-11-005.yaml | CAR |
| CAR-2013-01-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-01-002.yaml | CAR |

**Mitigation**

Restriction of Registry permissions can help. Ensure that the proper permissions are set for Registry hives to prevent users from changing these keys.

| Mitigation ID | Name | Description |
|---|---|---|
| M1024 | Restrict Registry Permissions | Some samples of REvil that were run in MITRE's lab made modifications to the Windows endpoint. To better protect endpoints within an organization, ensure that Registry permissions are in place to help prevent REvil ransomware from having an additional method of disabling or interfering with security services. |

### T1134.001 Access Token Manipulation: Token Impersonation/Theft

**Threat Detection**

If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the runas command. Detailed command-line logging is not enabled by default in Windows.

**Mitigation**

Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. Also define who can create a process-level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token.

Administrators should log in as standard users but run their tools with administrator privileges using the built-in access token manipulation command runas.

An adversary must already have administrator-level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.

| Mitigation ID | Name | Description |
|---|---|---|
| M1049 | Anti-virus/ Antimalware | As noted earlier, in some cases REvil will make an effort to run at the administrator level on the local system. To help protect against this, use a least privilege administrative model to restrict users and accounts on the local system to only those that require privileges. |

## Privilege Escalation

### Exploitation for Privilege Escalation

**Threat Detection**

Examining behavior on endpoint systems, such as abnormal process behavior (e.g., suspicious files written to disk, process injection attempts, etc.), and monitoring for presence or loading of known vulnerable drivers (e.g., Sysmon Event ID 6) that adversaries can exploit to execute in kernel mode, might help indicate successful compromise. Looking for activity that may indicate an adversary has gained higher privileges can be helpful as well.

**Mitigations**

Installing application sandboxing, keeping software up-to-date, and employing patch management for enterprise endpoints and servers can help. Blocking execution of known vulnerable drivers that can be exploited for kernel mode can help prevent execution of malicious files. Having a CTI platform to become aware of what types of threats and software exploits can be used against a specific environment will help with awareness and prioritization. Lastly, have a tool to mitigate exploitation behavior and control flow integrity checking.

### Access Token Manipulation: Create Process with Token

**Threat Detection**

Audit the command-line activity to search for the "runas" command, and also monitor for use of the Windows API for specific functions like DuplicateToken() and CreateProcessWithTokenW and correlate that activity with other suspicious behavior to reduce false positives.

**Mitigations**

Limiting permissions so users and user groups cannot create tokens can help; this can be accomplished through Group Policies (GPO). Defining who can create process-level tokens to local and network services will help limit privilege accounts and manage them. User account management can help restrict adversaries from gaining the higher privileges they need.

## Execution

### T1047 Windows Management Instrumentation

**Threat Detection**

Monitor network traffic for WMI connections, the use of WMI in environments that do not typically use WMI. Specific commands and parameters referencing "wmic" along with commands used for remote behavior may also be indicative of malicious activity.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2014-11-007 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-11-007.yaml | CAR |
| CAR-2014-12-001 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-12-001.yaml | CAR |
| CAR-2016-03-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2016-03-002.yaml | CAR |

**Mitigations**

Manage privileged accounts and restrict and/or disallow users from making remote connections using WMI.

### T1059.001 PowerShell

**Threat Detection**

PowerShell logging can be enabled to examine PowerShell execution details alongside other data. Monitor for loading and/or execution of artifacts associated with PowerShell assemblies, such as System.Management.Automation.dll. If PowerShell is not typically used in an environment, then looking for any PowerShell execution may be helpful. Changes in policy may also be beneficial. For ransomware, it might be helpful to look at detections that are also used for Impact techniques (e.g., Inhibit System Recovery), since PowerShell is likely being used to accomplish components of the ransomware attack.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2014-04-003 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-04-003.yaml | CAR |
| CAR-2014-11-004 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-11-004.yaml | CAR |

**Mitigations**

| Mitigation ID | Name | Description |
|---|---|---|
| M1049 | Anti-virus/ Antimalware | Windows 10 offers an AMSI that integrates with User Account Control, PowerShell, wscript.exe, cscript.exe, JavaScript, VBScript and Office VBA macros. An organization can use AMSI where appropriate to analyze commands as they are being processed to detect suspicious behavior. |
| M1045 | Code Signing | Ensure that a PowerShell policy is in place that only permits the execution of signed scripts. |
| M1042 | Disable or Remove Feature or Program | Where possible, disable the Windows Remote Management Service to prevent remote execution of PowerShell. |
| M1026 | Privileged Account Management | In instances where PowerShell is needed, restrict execution to Administrators only. |

### T1059.003 Windows Command Shell

**Threat Detection**

Depending on the job role, a baseline of what is normal for users should be in place, as some may require this as part of their routine tasks. Monitor processes and command-line arguments for script execution and subsequent behavior and see if the behavior relates to any other type of post-compromise events that are occurring on a system.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2014-11-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2014-11-002.yaml | CAR |
| CAR-2013-02-003 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-02-003.yaml | CAR |

**Mitigation**

Application control can be used when appropriate.

| Mitigation ID | Name | Description |
|---|---|---|
| M1038 | Execution Prevention | As part of a Least Privilege Administrative model restrict users' permissions to execute applications with administrative rights. |

### T1059.005 Visual Basic

**Threat Detection**

If VBS scripting is restricted for basic users, then any attempts related to it would be considered suspicious. Payloads and scripts should be captured at the file system to determine intent. Monitor for events like Office applications spawning processes, usage of the Windows Script Host (e.g., cscript.exe, wscript.exe), file activity involving VB payloads or scripts, and loading modules in VB languages (vbsscript.dll). It will likely occur alongside other potentially suspicious events, so monitor processes and command-line arguments for subsequent behavior.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2013-04-002 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-04-002.yaml | CAR |

**Mitigations**

To help mitigate this, anti-virus can be used to quarantine suspicious files. Restrictions can be set on unnecessary VB components and on scripting extensions so that they cannot be used during the exploitation process. Lastly, application control can be used where appropriate.

| Mitigation ID | Name | Description |
|---|---|---|
| M1049 | Anti-virus/ Antimalware | Windows 10 offers an AMSI that integrates with User Account Control, PowerShell, wscript.exe, cscript.exe, JavaScript, VBScript, and Office VBA macros. An organization can use AMSI where appropriate to analyze commands as they are being processed to detect suspicious behavior. |

### T1106 Native API

**Threat Detection**

API monitoring alongside correlation of other events with behavior surrounding API function calls will provide context to determine if events are malicious.

**Mitigations**

Identify and block and malicious software that can be executed by using application control tools (e.g., Windows Defender Application Control,. AppLocker). Also, software restriction policies can be established where appropriate.

| Mitigation ID | Name | Description |
|---|---|---|
| M1038 | Execution Prevention | There have been instances where Windows Defender has detected ransomware samples prior to execution in MITRE's lab. Organizations should have tools deployed to their endpoints that detect and block the execution of malicious software. |

### T1204.002 User Execution: Malicious File

**Threat Detection**

Monitor the execution of and command-line arguments for applications that require user interaction that an adversary may use to gain initial access. This includes compression applications, such as those for zip files, that can be used to deobfuscate/decode files or information [T1140] in payloads.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2021-05-002 | Windows | https://github.com/mitre-attack/car/blob/84e292a062ae6eecd1425db36bfc94a773669f5c/analytics/CAR-2021-05-002.yaml | CAR |

**Mitigations**

Application control may be able to prevent the running of executables masquerading as other files. Use user training to bring awareness to common phishing and spearphishing techniques and raise suspicion for potentially malicious events.

| Mitigation ID | Name | Description |
|---|---|---|
| M1038 | Execution Prevention | There have been instances where Windows Defender has detected ransomware samples prior to execution in MITRE's lab. Organizations should have tools deployed to their endpoints that detect and block the execution of malicious software. |
| M1017 | User Training | Establishing a baseline security training program within an organization for all users will educate them on basic security practices and inform them not to download and execute email attachments. |

## Command and Control

### T1105 Ingress Tool Transfer

**Threat Detection**

Network data should be analyzed for any unusual data flows or network communications that have not been seen before. Packet content analysis can also be helpful for detecting communications that are different from expected behavior from specific ports or protocols. File creation and files transferred into the network with utilities like File Transfer Protocol that are unusual should also be inspected.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2013-05-003 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-05-003.yaml | CAR |
| CAR-2013-05-005 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-05-005.yaml | CAR |
| CAR-2013-07-001 | Windows | https://github.com/mitre-attack/car/blob/9d3155c48dee3b8881c5629cc96730accc05ec9c/analytics/CAR-2013-07-001.yaml | CAR |

**Mitigations**

Network intrusion prevention systems can help identify ransomware and other unusual data being transferred over the network.

| Mitigation ID | Name | Description |
|---|---|---|
| M1031 | Network Intrusion Prevention | Organizations must have an intrusion prevention system in place for all endpoints that house sensitive data. As was mentioned in Section 4.2, knowing when unusual networking events occur outside of expected workflows can provide insight into the early stages of an attack. |

### T1573.002 Asymmetric Cryptography

**Threat Detection**

Network data can be analyzed for uncommon data flows, and processes using the network that have not been seen before should be looked at. Packet-based analysis that can detect whether communications are expected from specific protocols and ports will also be useful. Secure Sockets Layer/Transport Layer Security (SSL/TLS) inspection can also help detect C2 traffic within encrypted communication channels.

**Mitigations**

Network intrusion detection and prevention systems can be used to identify network signatures and mitigate activity at the network level. Adding in SSL/TLS inspection can help see contents of encrypted sessions to look for indicators of ransomware communications.

| Mitigation ID | Name | Description |
|---|---|---|
| M1031 | Network Intrusion Prevention | Organizations must have an intrusion prevention system in place for all endpoints that house sensitive data. As was mentioned in Section 4.2, knowing when unusual networking events occur outside of expected workflows can provide insight into the early stages of an attack. |
| M1020 | SSL/TLS Inspection | Inspecting outbound SSL/TLS communication on sensitive systems allows an organization to detect indications of malware communication. |

### T1071.001 Web Protocols

**Threat Detection**

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application-layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.

**Mitigations**

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.

| Mitigation ID | Name | Description |
|---|---|---|
| M1031 | Network Intrusion Prevention | Several samples of REvil were investigated in MITRE's lab and initiated a series of DNS requests to specific URLs immediately after being executed. Having networking alerts in place that can detect similar behavior to that observed in MITRE's lab can be an early indicator that a ransomware attack is underway. |

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| c75309a3-59f8-4a8d-9c2c-4c927ad50555 | Windows | https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_exfiltration_and_tunneling_tools_execution.yml | Sigma |
| c8557060-9221-4448-8794-96320e6f3e74 | Windows | https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/proxy/proxy_powershell_ua.yml | Sigma |

## Exfiltration

### T1041 Exfiltration over C2 Channel

**Threat Detection**

Analyze network data for uncommon data flows and packet contents to detect communications that do not follow expected protocol behavior.

**Mitigations**

Network intrusion detection and prevention systems can be used to identify network signatures and mitigate activity at the network level. Signatures can be unique indicators within protocols that are based off the obfuscation technique used by a tool or adversary.

| Mitigation ID | Name | Description |
|---|---|---|
| M1031 | Network Intrusion Prevention | Network intrusion detection and prevention systems can be used to identify network signatures and mitigate activity at the network level. Signatures can be unique indicators within protocols that are based off the obfuscation technique used by a tool or adversary. |

.

## Impact

For this section, emphasis should be on prevention, making sure the proper mitigations are in place. While detection of ransomware is still important, it often makes itself known through the ransom demand, so detection of ransomware can help mostly before encryption has begun, and is less helpful once it has already occurred. Nonetheless, there is value to be gained from understanding an entire ransomware attack to be able to enhance defenses.

### T1489 Service Stop

**Threat Detection**

For detection, monitor processes and command-line arguments to see if critical processes are being terminated. The registry also is accountable for changes made to services or startup programs, so verify that they are being monitored.

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| eb87818d-db5d-49cc-a987-d5da331fbd90 | Windows | hhttps://github.com/SigmaHQ/sigma/blob/eb406ba36fc607986970c09e53058af412093647/rules/windows/process_creation/win_service_stop.yml | Sigma |

**Mitigations**

Ensure that the proper registry and process and file permissions are in place so that adversaries cannot disable critical services. Limit privileges of user accounts and groups so only authorized administrators can change service configurations. Lastly, network segmentation can help detect intrusions, as it isolates critical systems and resources from being exposed to the internal network.

| Mitigation ID | Name | Description |
|---|---|---|
| M1024 | Restrict Registry Permissions | Some samples of REvil that were run in MITRE's lab made modifications to the Windows endpoint. To better protect endpoints within an organization, ensure that Registry permissions are in place to help prevent REvil ransomware from having an additional method of disabling or interfering with security services. |
| M1018 | User Account Management | Ensure that user permissions are set properly on all endpoints within an organization. REvil will look for ways to elevate its privileges, and having proper user permissions in place can assist in preventing REvil from disabling or interfering with security services. |
| M1022 | Restrict File and Directory Permissions | Ransomware will often attempt to interfere with services to further its access during an attack. Ensure that limitations are in place for user accounts and groups and that only administrators can make modifications to service configurations. |
| M1030 | Network Segmentation | Intrusion detection, analysis, and response systems should be run on a separate network from the production environment. Doing so will lessen the chances that a ransomware attack can interfere with critical response functions. |

## T1490 Inhibit System Recovery

**Threat Detection**

More general areas for detection would be to monitor processes and execution of command-line parameters, as well as the status of services involved in system recovery. To detect this technique, a security team should monitor processes and command-line parameters that include "vssadmin," "wbadmin," and "bcdedit." The registry can also track changes made to system recovery features, so monitor for changes made there.

For Windows event logs, Event ID 524 can indicate that a system catalog was deleted and might show suspicious activity. Monitor the status of services involved with system recovery. The Registry should also be monitored for changes with system recovery features (e.g., HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\DisableLocalPage).

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| CAR-2020-04-001 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2020-04-001.yaml | CAR |
| CAR-2021-01-009 | Windows | https://github.com/mitre-attack/car/blob/eaf711f53b092cb70b8accc88b7c2cd197b5a074/analytics/CAR-2021-01-009.yaml | CAR |
| CAR-2021-05-003 | Windows | https://github.com/mitre-attack/car/blob/84e292a062ae6eecd1425db36bfc94a773669f5c/analytics/CAR-2021-05-003.yaml | CAR |
| 87df9ee1-5416-453a-8a08-e8d4a51e9ce1 | Windows | https://github.com/SigmaHQ/sigma/blob/dfd9e6d8f05ec08cd3c0d391ad6d6104a3542666/rules/windows/powershell/powershell_delete_volume_shadow_copies.yml | Sigma |
| b5ea4bfe-a1b2-421f-9d47-22a75a6f2921 | Windows | https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/impact_volume_shadow_copy_deletion_via_vssadmin.toml | Elastic |

**Mitigations**

The most basic mitigations recommended are data backups and having a disaster recovery plan in place that contains procedures for regular data backups that can be used for restoration. Backups should be stored off system, especially to guard against a ransomware attack where the data is at risk of being destroyed. Consider technical controls to prevent disabling of services or deletion of files that are involved in system recovery.

## T1486 Data Encrypted for Impact

**Threat Detection**

Monitor and search for large quantities of file modifications in user directories as well as processes. Systems that centralize file storage in an organization are the best place to implement this type of detection. In some cases, monitoring for unusual kernel driver installation can help detect data being encrypted.

**Mitigations**

The main mitigation is to implement a data backup and recovery plan. The backups should be stored off system and protected from common methods that ransomware operators can use to gain access to destroy backups. It can also be beneficial to have multiple versions so that encrypted data does not overwrite the unencrypted data if detection takes too long.

| Mitigation ID | Name | Description |
|---|---|---|
| M1053 | Data Backup | Organizations must have a disaster recovery plan in place and practice it, ideally on a quarterly basis. A process to test data backups used in an organization's disaster recovery plan must be in place as well. An organization's incident response team will need to be aware of both the disaster recovery plan and how to initiate it. |

| Analytic ID | OS | URL | Source Repository |
|---|---|---|---|
| 97919310-06a7-482c-9639-92b67ed63cf8 | Windows | https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/file_event/win_susp_multiple_files_renamed_or_deleted.yml | Sigma |

## T1485 Data Destruction

**Threat Detection**

A common tool adversaries will use to accomplish this is SDelete, which results in a complete destruction of data that cannot be recovered, since it overwrites the contents vs. sending it to a recycle bin with the regular delete command. Monitor for usage of this tool or any tools similar to it. Examining high-file modification activity and creation of suspicious files will aid in detection as well.

**Mitigation**

If an organization has not conducted a threat assessment (e.g., threat modeling) of its systems, it is imperative to conduct it, as this will help uncover potential vulnerabilities in the organization's attack surface. This exercise can also assist an organization with the creation of an incident response plan for a potential ransomware attack, by identifying high-value targets and systems that contain valuable data.

For systems that contain sensitive information, healthcare organizations need to have an established disaster recovery plan in place that includes how to respond to a ransomware attack. This plan should be practiced on a regular basis (at least biannually).

At a minimum, an organization must have a playbook in place that outlines how they will respond to a ransomware attack. This playbook should also be practiced on a regular basis so individuals are prepared in the event they need to respond.

Regardless of the approach an organization takes, valuable data should always be backed up and readily available to use in the incident response process that it has chosen.

### T1491.001 Defacement: Internal Defacement

**Threat Detection**
Monitor application logs for abnormal behavior that may indicate attempted or successful exploitations.

**Mitigation**
IT disaster recovery plans can contain procedures for restoring services and systems.

## Conclusion

With the increased impact and success of ransomware, it comes as no surprise that there is growing interest by adversary groups to attempt these types of attacks. REvil ransomware, along with many others, continues to bring about new and emerging threats to the healthcare sector. Detection and mitigations strategies may change as time goes on, but the most important thing is that organizations start prevention, implement detections, and prepare response plans as early as they can.

# References


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. Saavedra-Morales, J. (2019, 10 20). *McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – Crescendo*. Retrieved October 20, 2019 from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/.
12. Dept. of Treasury. (2021, 09 21). *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. Retrieved November 22, 2021 from https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
13. Orkhan, M., et al. (2019, 07 03). *Sodin ransomware exploits Windows vulnerability and processor architecture*. Retrieved November 22, 2021 from https://securelist.com/sodin-ransomware/91473/

# Appendix A: REvil Technique Timelines from Public Threat Reporting

The techniques shown below are gathered from public threat reporting coverage of the REvil ransomware variant. The techniques are presented in the order in which REvil uses them in the report to showcase a sequential timeline of infection.

**Source 1:** https://www.secureworks.com/research/revil-sodinokibi-ransomware

| 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 privilege using LPE exploit if this key is enable+D5d, CVE-2018-8453 |
| privilege escalation | T1068 | exploitation for privilege escalation | Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. | Elevate privilege using LPE exploit if this key is enabled, CVE-2018-8453 |
| 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 |
| privilege escalation | ASdfghjkl;' 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 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 execute a new instance of itself with administrative rights. |
| 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. |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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. |
| impact | T1489 | service stop | Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. | Terminate blacklisted processes to eliminate potential resource conflicts that could impede REvil's ability to wipe or encrypt files |
| execution | T1059.003 | command and scripting interpreter: windows command shell | Adversaries may abuse the Windows command shell for execution. | Uses cmd.exe to perform inhibit system recovery technique |
| 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. | To make sure the compromised system is unable to restore from backup, it deletes shadow copies and disables recovery mode by executing the following command: cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures |
| 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 the key is set to true, REvil will wipe the content of blacklisted folders and erase them. |
| 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. | Iterates through all folders and files residing on local fixed drives and verifies they are not whitelisted |

| 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. | Begins the encryption process using the Salsa20 stream cipher, reads the file contents to a buffer, encrypts the contents of the buffer, writes the encrypted contents of buffer to original file, overwriting existing file, and renames the original file with previously generated random extension |
| impact | T1491.001 | defacement: internal defacement | Adversaries may deface systems internal to an organization in an attempt to intimidate or mislead users. | Configure background image text once the encryption process occurs with a text along the lines of "You are infected!" and it will explain where the user can go to read instructions in the text file on the system. This makes the victim aware of the compromise. |
| discovery | T1012 | query registry | Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. | It does another check to the Registry to confirm whether C2 communication should take place |
| 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 to send information using the HTTPS protocol |
| exfiltration | T1041 | exfiltration over C2 channel | Adversaries may steal data by exfiltrating it over an existing C2 channel. | Sends host profile and malware information to C2 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. | Sends encrypted stat data to C2 server |

**Source 2:** https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| defense evasion | T1140 | deobfuscate/decode information | Adversaries may require separate mechanisms to decode or deobfuscate information, depending on how they intend to use it. | Decrypts strings it uses during execution at runtime |
| execution | T1106 | native API | Adversaries may directly interact with the native OS API to execute behaviors. | Dynamically resolves imports needed to function properly, resolves the correct API, etc. Uses GetProcAddress API. |
| 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. | Attempts to access and search for 2 separate registry keys, depending on whether the first attempt is successful |
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Grabs information needed for letter (CPU info, serial number, hardware ID) |
| 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. | Information obtained from host is encrypted |
| 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. | Modifies the discovered registry keys by adding the encrypted data found there |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Checks the system language, keyboard layout |
| impact | T1489 | service stop | Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. | Stop and delete services if name matches list of service in JSON config list. Terminates all processes. |
| execution | T1059.003 | command and scripting interpreter: windows command shell | Adversaries may abuse the Windows command shell for execution | If it is windows 5.1 and earlier, uses the cmd.exe shell to perform inhibit system recovery |
| execution | T1059.001 | command and scripting interpreter: powershell | Adversaries may abuse PowerShell commands and scripts for execution. | If windows version 5.2 and later, it uses PowerShell Get-WmiObject Win32_Shadowcopy |
| 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. | Deletes volume shade copies, depending on Windows version |
| 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. | Before encryption, it determines if names match whitelist config files/folders/extensions |
| 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 uses multithreading I/O completion ports and encrypts files simultaneously |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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 | Encrypts all important data it stores in the registry |
| impact | T1491.001 | Defacement: internal defacement | Adversaries may deface systems internal to an organization in an attempt to intimidate or mislead users. | REvil generates a bitmap image and sets it as the desktop background |
| 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. | Determines whether needs to communicate with C2 server |
| defense evasion | T1070.004 | indicator removal on host: file deletion | Adversaries may delete files left behind by the actions of their intrusion activity. | It marks its binary code for deletion during next reboot and terminates execution |

**Source 3:** https://blogs.blackberry.com/en/2019/07/threat-spotlight-sodinokibi-ransomware

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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. | All strings and configuration are encrypted with RC4 before use |
| defense evasion | T1140 | deobfuscate/decode files or information | Adversaries may require separate mechanisms to decode or deobfuscate information, depending on how they intend to use it. | Decrypts embedded configuration |
| privilege escalation | T1068 | exploitation for privilege escalation | Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. | CVE-2018-8453 to gain system privileges |
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Gathers basic system info, checks language and keyboard layout |
| 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. | Gathers the username |
| 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. | Encrypts found 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 | Stores encrypted system information and added to the registry |

| 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. | Terminates processes specified by prc value |
| execution | T1059.003 | command and scripting interpreter: windows command shell | Adversaries may abuse the Windows command shell for execution | Launch cmd.exe to perform inhibit system recovery |
| 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 | Delete volume shadow copies |
| 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. | Makes sure files and folders that are whitelisted are ignored, has an exception list |
| 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. | Encrypts files on the system using Salsa20 |
| impact | T1491.001 | defacement: internal defacement | Adversaries may deface systems internal to an organization in an attempt to intimidate or mislead users. | Background wallpaper will be set with ransom note |
| 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, all the files and folders listed under wfld will be zeroed out and deleted |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
| --- | --- | --- | --- | --- |
| command and control | T1041 | exfiltration over C2 channel | Adversaries may steal data by exfiltrating it over an existing C2 channel. | If flag is set, ransomware will broadcast victim's system information to a range of domains |
| 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 |
| 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. | Does not rely on network communication, but has the option functionality to reach out to C2 if net parameter is set |

**Source 4:** https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| defense evasion | T1140 | deobfuscate/ decode files or information | Adversaries may require separate mechanisms to decode or deobfuscate information, depending on how they intend to use it. | Decrypts strings in configuration before execution |
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Check operating system, OS version |
| execution | T1106 | native API | Adversaries may directly interact with the native OS API to execute behaviors | Uses built-in functions like GetSystemNativeInfoW before executing shellcode |
| 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 | Obtain process token of execution privilege and relaunch the process using runas |
| 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. | User information is obfuscated |
| 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. | Collects user name from the host machine |
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Collects additional information like the machine name, produce name, OS name |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| discovery | T1069.002 | permission groups discovery: domain groups | Adversaries may attempt to find domain-level groups and permission settings. | Collects domain group information |
| discovery | T1082 | system information discovery | Adversaries may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. | Checks the system language of the machine to determine whether to continue execution based on blacklisted language set |
| 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. | Stores the data in Windows Registry "SOFTWARE\recfg" |
| impact | T1489 | service stop | Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. | Search all processes in list and terminate them in a loop |
| execution | T1059.003 | command and scripting interpreter: Windows command shell | Adversaries may abuse the Windows command shell for execution | It executes inhibit system recovery with the command shell |
| 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. | 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 |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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 the field is set to "true" it will destroy and delete all files with random trash or with 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. | Enumeration of files and folders, avoiding whitelisted folders and names of files/extensions |
| 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. | Encryption of flagged files and dropping ransom note in each folder |
| impact | T1491.001 | defacement: internal defacement | Adversaries may deface systems internal to an organization in an attempt to intimidate or mislead users. | After encryption, it will create the image of the desktop in runtime with the text that comes with the config file prepared with the random extension |
| 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 field "net" from the config is set to "true" then it will start sending POST message to the list of domains in the config file |

**Source 5:** https://www.picussecurity.com/resource/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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 enable content, which launches the code hidden in macros |
| execution | T1059.005 | command and scripting interpreter: Visual Basic | Adversaries may abuse Visual Basic (VB) for execution. | Has embedded VBA macro codes into modules and functions |
| 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. | REvil has obfuscated modules/functions |
| command and control | T1105 | ingress tool transfer | Adversaries may transfer tools or other files from an external system into a compromised environment. | REvil uses function to download bits from the internet, saves them to a file (URLDownloadToFile) |
| defense evasion | T1036.005 | masqureading: match legitimate name or location | Adversaries may match or approximate the name or location of legitimate files or resources when naming/ placing them. | REvil's artifacts usually mimic the names of known executables |
| execution | T1059.003 | command and scripting interpreter: Windows command shell | Adversaries may abuse the Windows command shell for execution. | Uses cmd.exe to launch inhibit system recovery |
| 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. | Runs vssadmin.exe to delete all volume shadow copies on system to prevent recovery |

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | TECHNIQUE DESCRIPTION | PROCEDURE EXAMPLE(S) |
|---|---|---|---|---|
| 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. | Uses bcdedit.exe twice to disable automatic windows recovery features by modifying boot configuration data |
| 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. | Encrypts files and adds ransom extension |

***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®