Ransomware: A Beginner's Guide to Threat Detection

by Darren Mccutchen, netwitness.com, Aug 11, 2021
Republished by techrepublic.com, 5/22/22

If you have been following the news, you'll have most certainly been bombarded by the term ransomware. Almost every week, another large company publicly discloses being impacted by this type of attack. Due to the increased awareness of ransomware, one may think that this is a new phenomenon. But it's not. (The first widely distributed ransomware attack, the AIDS Trojan, was delivered via floppy disk in 1989.) Ransomware is a class of malware that, once executed on a victim's computer, renders the system and/or its data inaccessible until a ransom payment is completed. This is typically achieved by either:

What exactly is ransomware?

1. Locker ransomware: prevents the user from using basic system functions, making the computer inoperable. The goal of locker ransomware is to prevent system access, not destroy data.
2. Crypto ransomware: identifies and encrypts the contents of entire drives and/or specific valuable data on the victim system. Beginning with CryptoLocker in 2013, most modern ransomware attacks involve some form of data encryption.

What does ransomware cost companies?

With improvements in encryption algorithms, the introduction of crypto payments, and easier distribution, the major 1989 to today is financial:

In 2019, costs associated with ransomware attacks passed $7.5 billion. (Source)

In 2021, medium-sized organizations paid out an average of $170,404 for ransom demands. (Source)

Over the last three years, requested ransom fees have increased 4,000%, going from $5,000 in 2018 to around $200,000 in 2020.

In 2021 alone, there have been several major high-profile ransomware attacks resulting in hundreds of millions of dollars lost:

CNA:

US-based insurance company CNA paid a $40 million ransom payment after being attacked with Phoenix CryptoLocker ransomware, created by the group Evil Corp. More than 15,000 devices on the CNA network were impacted by the ransomware, including the systems of remote workers connected via VPN. CNA was forced to take many systems and its website offline for a short period of time.

JBS USA.

On June 1, meat processing company JBS suffered a large-scale ransomware attack at the hands of the REvil (a.k.a. Sodinokibi) group, forcing the company to shutdown plants in Australia and Brazil. JBS ended up paying $11 million in Bitcoin as a ransom payment. Post-compromise analysis revealed that REvil was able to conduct a three-month data exfiltration campaign (March 1–May 29, 2021) before any data encryption occurred. (Source)

Colonial Pipeline Company.

In late April, the DarkSide group was able to deploy ransomware on the Colonial operation al network using leaked VPN credentials. As a result, Colonial was forced to shut down the entire pipeline for five days, resulting in massive gas shortages and higher fuel prices. After being threatened with a data leak using 100GB of data that DarkSide was able to exfiltrate, Colonial ended up paying a $4.4 million ransom

How is ransomware distributed?

From the first widely distributed attacks using a floppy disk, to the use of botnets in the mid to late 2000s, ransomware distribution methods have evolved over the years. The most recent ransomware families and their associated variants most frequently employ the following techniques:

Phishing: Emails containing malicious links or attachments are one of the most common delivery techniques for ransomware payloads. According to Proofpoint's State of Phish report, 47% of successful phishing campaigns resulted in some form of ransomware infection. Ryuk, a ransomware developed by Russian hacking group WIZARD SPIDER, is primarily delivered as a second-stage infection after initial Trickbot infection via malicious email attachments

Automated recon scans: This method employs open internet scans, using services such as Shodan, to identify internet facing systems with open ports (ex: TCP/3389-Remote Desktop Protocol) or running unpatched exploitable versions of software. CloP, a now defunct ransomware group, was able to exploit two zero-days, CVE-2021-27102 and CVE-2021-27104, which allowed for remote code execution within unpatched Accellion FTA instances

Ransomware-as-a-Service (RaaS): A newer method of distribution, RaaS outsources the initial compromise of corporate systems (some will even outsource all actions up to ransom collection), with some form of subscription or profit splitting. While there are multiple revenue models for RaaS, some of the larger ransomware families like DopplePaymer, Maze, and NetWalker are operating under the Affiliate model. In the Affiliate model, a ransomware provider will develop/maintain the malware's code in addition to setting up the associated infrastructure (payment portals, unique IDs, troubleshooting support, data leak sites). These groups will then recruit "affiliates" to deliver the ransomware payload to targeted victims. Once profits have been paid, the ransom group and the affiliates will split the profits.

What are the stages of a ransomware infection?

Once a target has been identified, the ransomware lifecycle can be observed through the following stages:

01 Initial Access/Distribution. In addition to the previously detailed methods of distribution, ransomware can infect victims via most well-known malware delivery mechanisms such as drive-by-downloads, mishandling of malicious data, third-party compromise, or as a secondary stage of previously downloaded malware. Due to the wide range of compromise vectors being like other types of malware, it is difficult to categorize an attack as solely ransomware during this stage. This is the beginning of a ransomware attack.

02 Infection. Now that the dropper file is on the victim machine, a malicious executable (or another file) containing the ransomware payload is downloaded This can be completed by making a call to a hardcoded URL or as an automated second stage of the initial infection vector. At this point you may see network traffic to suspicious IPs or domains that hold the malicious files. Once downloaded, the executable is typically placed in a local Windows %temp% directory (may also end up in the root or a subdirectory of C:\ such as C:\Windows), the original dropper file is removed, and the downloaded malicious file is executed.

03 Payload Staging. At this point, the ransomware begins to set itself up for successful execution. The main goal of this stage is to ensure completion of ransomware attack and persistence through system shutdowns. Some actions the ransomware may take during this stage include but are not limited to: At this point, the ransomware begins to set itself up for successful execution.

The main goal of this stage is to ensure completion of ransomware attack and persistence through system shutdowns. Some actions the ransomware may take during this stage include but are not limited to: At this point, the ransomware begins to set itself up for successful execution.

- Running checks to see if ransomware has previously been deployed on the system
- Checking, adding, and modifying Registry values
- Discovering user accounts and their associated privileges
- Attempting privilege escalation
- Identifying mapped network shares
- Deleting system backup

04 Scanning Once the ransomware payload has completed staging the environment, it begins identifying files to encrypt. This can be completed by using hardcoded list of files to target or avoid. In certain human operated ransomware campaigns, adversaries may manually identify highly valuable data to encrypt. In other cases, ransomware will encrypt an entire drive (Petya). Using the network mapping data gathered during "Payload Staging", ransomware can remotely identify systems/drives/files to target as well. Some recent ransomware variants will also look to encrypt data on any connected cloud storage providers.

- Disabling recovery tools
- Compiling encryption/decryption keys
- Adjusting system boot settings (some variants reboot victims in 'Safe Mode')
- Depending on the malware variant, C2 communication may be established.

05 Data Encryption: Files will be encrypted in one of two ways:

- Encrypted data will be written over the original data and data will be renamed.
- A copy of original data will be encrypted, and the original will be deleted.

Different ransomware families may prefer specific encryption algorithms or a combination of many. An example of this is in the Kaseya Supply Chain attack, in which REvil ransomware used a combination of Curve25519 (asymmetric) and Salsa20 (symmetric) encryption algorithms to encrypt target files. At some point either immediately prior, during, or after, encrypted files will be renamed and appended with a ransomware identifying hardcoded or dynamically generated file extension. With the target data identified, ransomware will begin encrypting. Encrypted data will be written over the original data and data will be renamed A copy of original data will be encrypted, and the original will be deleted

06 Ransom Demand: For any systems impacted by data encryption, a ransom note will be generated. This can be thought of as a "calling card" for the adversary. Notes can be dropped into a single directory, every directory that holds encrypted files, or as a "lock screen" on victim desktops. Typically, these notes will include characteristics (ransom note title, specific language, or direct mention of group) that informs the victim who attacked them. Ransom notes for specific ransomware families tend to be the same across many variants. Ransom notes will include the monetary demand in some form of crypto currency, how to access the payment portal, and a point of contact. Once paid, a private key is provided to the victim, however, there is no guarantee that the key will properly decrypt the targeted data. According to Sophos, 92% of victims lost at least some data, and more than 50% of them lost at least a third of their precious files, despite paying.

What are common behaviors of ransomware families?

With numerous ransomware families and their associated variants being actively exploited in the wild, cybersecurity professionals need a set of common criteria to identify, respond, and mitigate attacks more easily. Some of the methods we've witnessed across multiple ransomware attacks include:

- Privilege escalation attempts prior to lateral movement
- Disabling of security tools and the killing of specific system processes
- Deletion of Volume Shadow Copy (via vssadmin, WMI, or other)
- Recovery prevention via BCDedit
- Preference for remote encryption of mapped network drives from 1 or 2 infected hosts
- Encryption of files (Overwrite vs. Copy/Delete Method)
- Renaming of files
- Creation of a ransom note

Not every ransomware variant will display every one of these traits. However some combination of these common behaviors will be present in most ransomware attacks.

How can you better detect ransomware?

Using network and endpoint data, these are the ransomware red flags to look for:

1 Large number of files renamed in short period of time
2 Accessing and disabling of services/processes/applications that could detect execution of ransomware payloads
3 System backups, recovery partitions, and volume shadow copies deleted
4 System event logs disabled or deleted
Example Command-Line Arguments:

- "C:\Windows\System32\wevtutil.exe" cl Security
- "C:\Windows\System32\wevtutil.exe" cl System
- "C:\Windows\System32\wevtutil.exe" cl Application
- "C:\Windows\System32\wevtutil.exe" cl Setup

5 Ransom note naming conventions (only effective in stopping ongoing attack)

This is not a comprehensive list but should provide a starting point for detection of characteristics associated with a ransomware attack.