RELIAQUEST

Threat Advisory Report: Ransomware

Published: 04/20/2020

Introduction

Ransomware has become one of the most popular and destructive attacks in cyber security in recent years. Instead of stealing data as in most other attacks, the goal of ransomware is to hold the user's data hostage by making it unusable until a ransom fee is paid. This is accomplished by encrypting the victim's machine with an encryption key that the attackers then offer to sell back to the victim in exchange for cryptocurrency. The attack is easy once attackers have a foothold and requires little effort to execute, making this method much more cost efficient than other attacks. While ransomware can be thwarted by simply replacing the encrypted machine with a backup image, many organizations do not have the backups and are increasingly paying the ransom rather than accepting the massive data loss, increasing the success rate and popularity of this attack.

By knowing the techniques used by ransomware, it is possible to implement controls and detections to prevent ransomware infections, or at least limit its spread in the organization.

Technique Timeline

Initial Access

Before ransomware can begin encrypting files, it first needs to be present on the victim host. There are multiple techniques used by ransomware operators to infect their targets:

T1193 - Spearphishing Attachment / T1192 – Spearphishing Link

Just like with any phishing attempt, the sender is trying to trick the recipient into clicking on a link or attachment to execute the attack. The link could direct to a site that exploits the user's browser to download the ransomware payload. The attachment could be the payload itself or a dropper that downloads the payload separately, such as a macro-enabled document. The Locky ransomware used this technique to infect organizations by sending malicious .docm attachments in phishing emails.

T1189 - Drive-by Compromise

A more indirect method, drive-by compromise attacks rely on users to visit a malicious website that automatically exploits the users' browser in order to download malware. The exploitation is usually accomplished by exploit kits that take advantage of vulnerabilities in browsers and applications such as Flash. To drive traffic to the malicious website, attackers may purchase ads to display on benign sites or send spam or phishing emails. The Maze ransomware authors bought ads for a fake cryptocurrency exchange site running the Fallout exploit kit to host their ransomware. Once the user visits the website, the ransomware payload is downloaded to their host.

T1133 - External Remote Services

Instead of waiting for user interaction, attackers may instead attempt to directly login to the target hosts and install the ransomware manually. Organizations often leave Remote Desktop Protocol (RDP) or other remote access services open to the internet where they are exposed to brute force and credential reuse attacks that exploit weak or nonexistent passwords. Once they have access, the attackers can move the ransomware payload to the compromised host and execute it. They can even reuse the credentials to pivot to other hosts inside the network and spread the ransomware infection further. The SamSam ransomware brute forced public RDP portals to spread into organizations.

Execution

Once the malicious files have reached the endpoint, the next critical step is getting those files to execute. The most common way for this to occur is through user intervention. However, once infected, there are other ways to execute malicious commands.

T1204 - User Execution

The first phase of execution is typically run by the user through an executable, DLL, or a macro-enabled document. This phase often connects to the attacker's C2 server and sends the encryption keys. Macro-enabled documents are frequently utilized as a downloader of another executable or the initiating connection to the C2 server. Once the victim is connected to the C2 server, the attacker can drop the executable that is used for carrying out encryption activity.

T1047 – Windows Management Instrumentation

Notable ransomware variants have utilized Windows Management Instrumentation Command-Line (WMIC) in order to delete Windows Shadow copies which is essentially a snapshot of data.

WannaCry, for example, has been observed running the command[1]:
cmd.exe /c vssadmin delete shadows /all /quiet & ***wmic shadowcopy delete*** *& bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet*

Persistence

Attackers will prefer to maintain persistence on a victim machine for control purposes. While it may not be necessary, it has been observed in several ransomware campaigns that attackers will implement techniques for persistence.

T1060 – Registry Run Keys / Startup Folder

In order to maintain persistence on the victim host, ransomware binaries with additional motives have often been observed to create or modify registry keys in the path:
HKCU\Software\Microsoft\CurrentVersion\Run\

Additionally, the disabling of critical Windows services is often performed through the registry, such as disabling Windows Task Manager:

HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr

[1] https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/

Impact

The ultimate goal for ransomware campaigns is to encrypt the data on the victim machines and demand a ransom from the victim.

T1486 – Data Encrypted for Impact

In the final phase, many valuable filetypes on the victim machine have been encrypted such as Office documents, PDFs, images, text, source code files, etc. Some variants of ransomware also encrypt system files, full disk partitions, and the Master Boot Record (MBR).

ReliaQuest Detect

As a function of GreyMatter, Detect is a comprehensive library that is designed to provide threat coverage across several technologies.

Email Security

Log source that analyzes emails and attachments for phishing attempts.

T1193 - Spearphishing Attachment / T1192 – Spearphishing Link

RQ-SL-000133-01 - Allowed Phishing Email

RQ-SM-000135-01 - Allowed Attachment with Executable Extension

Endpoint

Log sources that provide endpoint visibility, including anti-virus, EDR, FIM, and native operating systems.

T1486 – Data Encrypted for Impact

RQ-SH-000812-01 - File Encryption from Unsigned Process

RQ-SH-000576-01 - Shadow Copies Deleted

RQ-SH-000785-01 - Ransomware Instruction Filenames

T1204 - User Execution

RQ-SC-000129-03 - Ransomware AV Detection

RQ-SC-000514-01 - Threat File Hash Detected

Remote Access

Log sources that provide remote access, including VPN, VDI, and remote SSH or RDP services.

T1133 - External Remote Services

RQ-SM-000169-02 - Remote Brute Force Account Guessing

RQ-SL-000170-01 - Remote Brute Force Password Guessing

RQ-SL-000172-01 - Remote Login from High-Risk Country

RQ-SM-000173-01 - Successful Remote Brute Force

RQ-SH-000174-01 - Successful Authentication from Threat Host
RQ-000176-01 - Direct Inbound Successful Authentications

Forward Proxy

Log sources that analyze URLs and file downloads.

T1189 - Drive-by Compromise

RQ-SM-000180-01 - Executable File Downloaded from High-Risk Domain
RQ-SM-000191-01 - Executable File Downloaded from Hardcoded IP

T1204 - User Execution

RQ-SH-000182-02 - POST to Threat Domain

This report, and any information, analysis, or other observations noted in this informational release, is provided for informational purposes only. The information contained herein is derived from data that ReliaQuest, LLC ("ReliaQuest") believes to be reliable, however no warranties, representations, or guarantees, are made by ReliaQuest with regard to the accuracy, completeness, or suitability of such information. To the fullest extent allowed by applicable law, ReliaQuest fully disclaims and any all liability with respect to the content and/or use of this information, in any manner, by any third party. Any opinions expressed reflect the current judgment of ReliaQuest and may change without notice. ReliaQuest has no obligation to amend, modify, or update this report or to otherwise notify a reader or recipient thereof in the event that any matter stated herein, or any information, opinion, projection, forecast, or estimate set forth herein, changes or subsequently becomes inaccurate.