Threat Assessment: WastedLocker Ransomware

By Alex Hinchliffe, Doel Santos, Adrian McCabe, Robert Falcone

Published: 2020-07-30 · Archived: 2026-04-05 16:27:57 UTC

Executive Summary

Unit 42 has observed a recent uptick in WastedLocker ransomware activity, which has increased since the initial samples were analyzed by WildFire in May 2020. In light of this, together with recent media coverage around large U.S. corporations being targeted by the threat, we have created this general assessment of the ransomware. Full visualization of these techniques can be viewed in the Unit 42 Playbook Viewer.

WastedLocker is post-intrusion ransomware of the same ilk as Samsa, Maze, EKANS, Ryuk, BitPaymer and others. This type of ransomware differs from large-volume, victim-agnostic ransomware variants like WannaCry by targeting an organization perceived as having a large amount of assets, successfully breaching it, and then deploying specially crafted ransomware to as many systems as possible within that organization in a short timeframe to maximize impact and increase chances of receiving a much larger ransom payment.

On June 23, 2020, NCC Group published a report providing a detailed overview of the WastedLocker ransomware, including information on the group believed to be behind it, Evil Corp. In the past, this group has been responsible for the Dridex banking Trojan and other related threats and campaigns.

The Palo Alto Networks Threat Prevention subscription for the Next-Generation Firewall with WildFire and the Cortex XDR endpoint protection engine detects activity associated with this ransomware. Cortex XDR also contains an Anti-Ransomware Protection module, which targets encryption-based activities associated with ransomware. Additionally, AutoFocus customers can review activity associated with this threat with the following tag: WastedLocker.

Targeting

Using our threat intelligence platform, AutoFocus, Unit 42 has identified some possible targets for the actors behind WastedLocker. The majority of organizations are based in the U.S., which ties in with activity reported by Symantec on June 26, 2020. The organizations operate in various sectors, including professional and legal services, utilities and energy, manufacturing, wholesale and retail, high tech, engineering, pharma and life sciences, and transportation and logistics (including one transportation and logistics organization from the United Kingdom that appears to have operations in the U.S).

WastedLocker Attack Technical Overview

Note: This is only a high-level overview of the pertinent technical aspects of WastedLocker attacks. For a more in-depth technical analysis, including Indicators of Compromise (IoCs), see SentinelOne's blog, "WastedLocker Ransomware: Abusing ADS and NTFS File Attributes.".

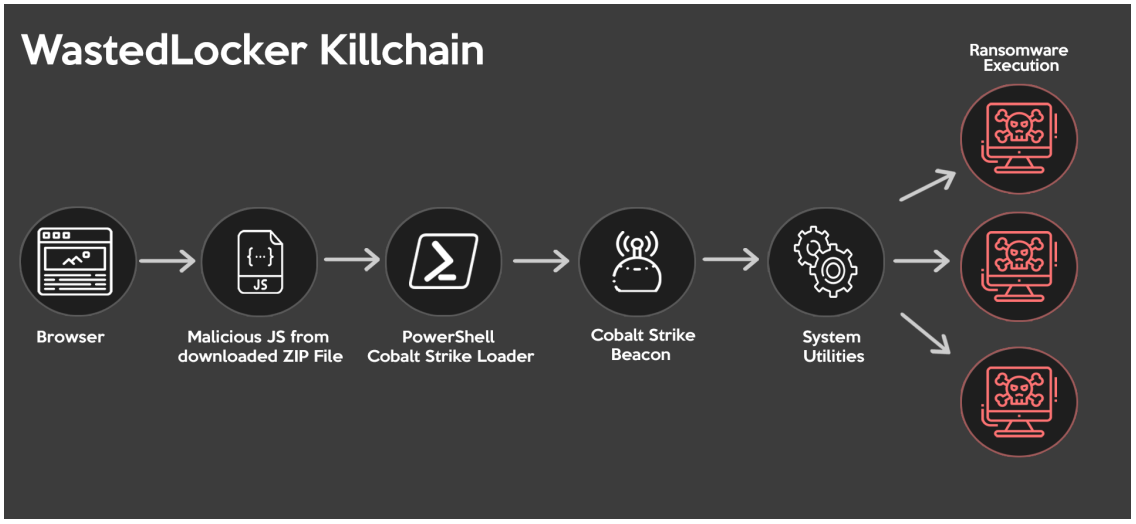

Figure 1. WastedLocker killchain

Initial Infection Vector

According to previously reported WastedLocker activity by Symantec, the most commonly observed initial infection mechanism for WastedLocker attacks are ZIP files (likely disguised as legitimate software updates) containing malicious SocGholish JavaScript framework loader components that profile the victim system and use PowerShell to ultimately deploy Cobalt Strike payloads.

While the full technical analysis of how the SocGholish framework operates is beyond the scope of this blog, an in-depth summary of its operation can be found in this post about fake browser update pages.

Lateral Movement

Once the Cobalt Strike payload is installed on a victim's machine, it is then used to move laterally through the victim's network and facilitate the identification of additional systems on which attackers can deploy their main payloads. (WastedLocker attackers have also been observed using legitimate Windows utilities such as Windows Management Instrumentation [WMI] and PsExec to do this as well.) Of particularly high value to targeted ransomware attackers are systems that directly affect a victim's customer-facing revenue-generating business operations, internal systems of high visibility and high use, and systems that contain (or facilitate the deployment of) system backups.

Final Payload

Finally, once sufficient reconnaissance of the victim's network has been conducted, the attackers move to deploy the WastedLocker ransomware payload using one or more system management utilities. (The exact mechanism is out of scope for this blog, but more details are available in SentinelOne's post.)

During execution on a target host, the ransomware will:

- Attempt to elevate execution privileges (if not already running as Administrator).
- Attempt to disable Windows Defender monitoring.
- Delete shadow copies/volume snapshots.

- Install itself as a service.

Once installed, the delivery of the payload is complete and files are overwritten. The ransomware mainly uses a `.<victim name>wasted` extension, though files containing ransom note details are appended with a `.<victim_name>wasted_info` extension.

The *.wasted_info ransom note files we have analyzed thus far resemble the following example where variable data is shown below between <> characters. The actor email addresses used can differ, and the domain names include the following (in most- to least-used order): PROTONMAIL.CH, AIRMAIL.CC, ECLIPSO.CH, TUTANOTA.COM and PROTONMAIL.COM

<victim name>

YOUR NETWORK IS ENCRYPTED NOW

USE <actor email 1> | <actor email 2> TO GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:

[begin_key]<base64 encoded public key>[end_key]

KEEP IT

Source: https://unit42.paloaltonetworks.com/wastedlocker/