

Threat spotlight: WastedLocker, customized ransomware

blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/

Pieter Arntz

July 10, 2020



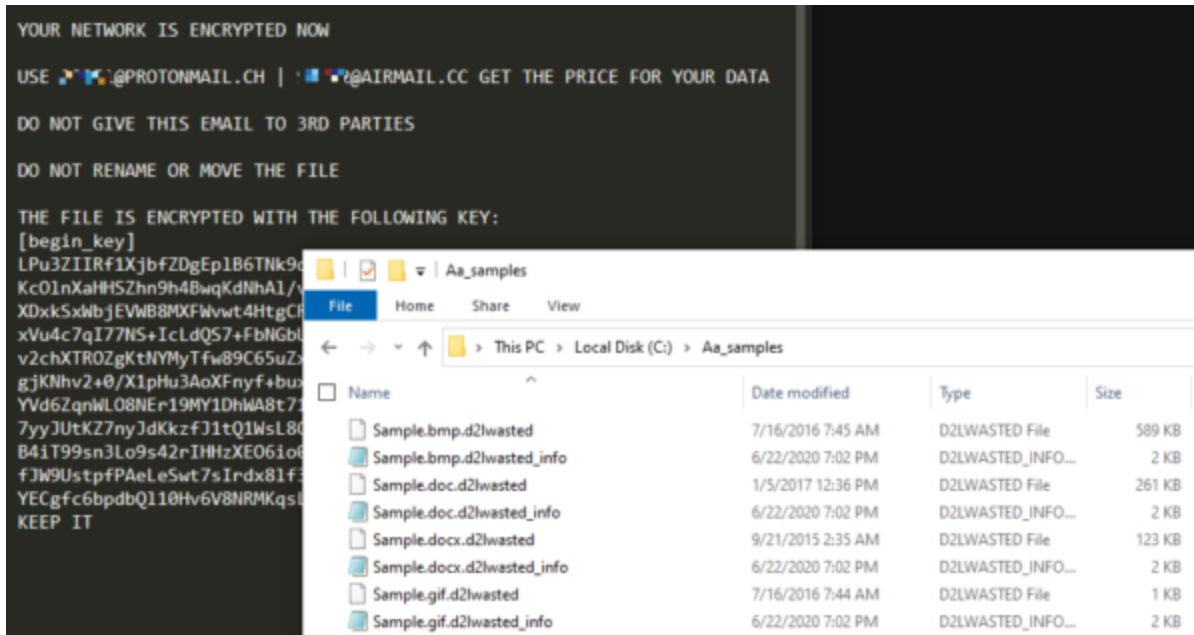
WastedLocker is a new ransomware operated by a malware exploitation gang commonly known as the Evil Corp gang. The same gang that is associated with [Dridex](#) and BitPaymer.

The attribution is not based on the malware variants as WastedLocker is very different from BitPaymer. What was kept was the ability to add specific modules for different targets.

The attacks performed using WastedLocker are highly targeted at very specific organizations. It is suspected that during a first penetration attempt an assessment of active defenses is made and the next attempt will be specifically designed to circumvent the active security software and other perimeter protection.

The ransomware name is derived from the filename it creates which includes an abbreviation of the victim's name and the string "wasted".

For each encrypted file, the attackers create a separate file that contains the ransomware note. The ransom note has the same name as the associated file with the addition of "_info".



The ransom demands are steep, ranging from \$500,000 to over \$10 million in Bitcoin. Given that the operators make every effort to go after any backups, some organizations may feel the need to pay up. Where other ransomware operators are adding the exfiltration and even auction of stolen data to their arsenal, the Evil Corp gang has shown no inclination in that direction yet.

Historically the Evil Corp gang targets mostly US organizations and it looks like they are staying on that track with a few victims in Europe. The main players in the group are believed to be Russian.

The importance of offline backups

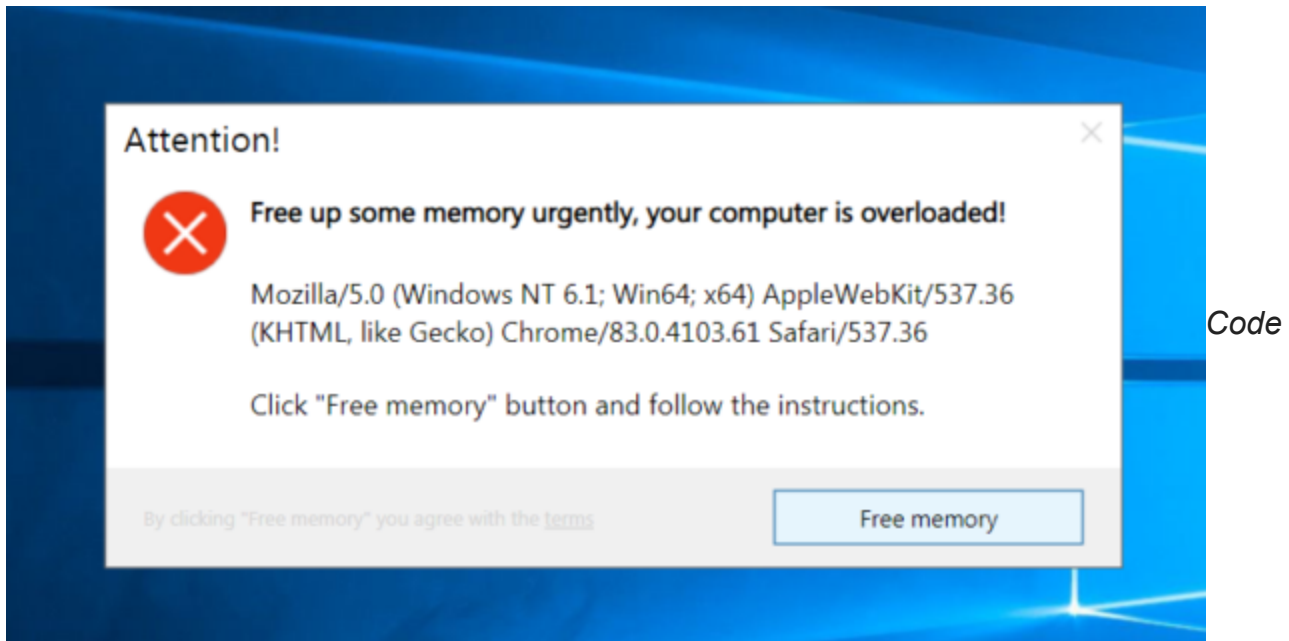
In general, we can state that if this gang has found an entrance into your network it will be impossible to stop them from encrypting at least part of your files. The only thing that can help you salvage your files in such a case is if you have either roll-back technology or a form of off-line backups. With online, or otherwise connected backups you run the chance of your backup files being encrypted as well, which makes the whole point of having them moot. Please note that the roll-back technologies are reliant on the activity of the processes monitoring your systems. And the danger exists that these processes will be on the target list of the ransomware gang. Meaning that these processes will be shut down once they gain access to your network.

As you may have noticed this is a very sophisticated and highly targeted type of ransomware. Which means that, given the ransom demands, most of the affected companies will have a dedicated cyber- security department. It is imperative that this staff is alert on the early warning signs of these attacks which may be indicated by breach attempts. At later stages more disruptive actions may be taken, such as disabled security software, dropped files, and deleted backups

Unlike other ransomware operators Evil Corp does not exfiltrate stolen data and publish or auction the data that belong to “clients” that are unwilling to pay the ransom.

Infection details

One of the methods found to date is the usage of fake software update alerts embedded in existing websites.



can be inserted on existing websites showing misleading information to prompt users and get them to run malware.

The malware from these websites is a penetration testing and exploration kit designed to create a foothold and gather information about the network. Historically Evil Corp has targeted file servers, database services, virtual machines, and cloud environments.

Once the exploration phase has completed the gang will drop the ransomware on the compromised systems.

The ransomware itself is custom built for each client so there is nothing to be gained by doing a full analysis. The attacks do have some commonalities though which we will discuss here.

- Deletes shadow copies, which are the default backups made by the Windows OS.
- The main executable for the ransomware is copied to the system folder and gets elevated permissions
- A service is created that runs during encryption.
- During encryption the encrypted files are renamed, and the ransom notes are created.
- A log file is created that lists the number of targeted files, the number of encrypted files, and the number of files that were not encrypted due to access rights issues.
- The service is stopped and deleted.

Overview

- WastedLocker has been actively deployed since May 2020.
- Evil Corp behind: this group previously associated to the Dridex malware and BitPaymer aka IECrypt aka FriedEx aka WastedLocker.
- Evil Corp has been using WastedLocker to request ransoms in the range of millions of USD, with some demands going above \$10 million.
- WastedLocker replaces BitPaymer in the group's operations.
- Technically, WastedLocker does not have much in common with BitPaymer
- The ransomware name is derived from the filename it creates which includes an abbreviation of the victim's name and the string 'wasted'.
- Encrypted files extension is set according to the targeted organisations name along with the prefix wasted
- Example: test.txt.orgnamewasted (encrypted data) and test.txt.orgnamewasted_info (ransomware note)
- No data theft and no leak site.
- Each ransomware victim has a custom build configured or compiled for them.
- Note contains: Protonmail and Tutanota email domains, as well as Eclipso and Airmail email addresses. The email addresses listed in the ransom messages are numeric – usually 5 digit numbers.

Infection highlights

- Delete shadow copies
- Copy the ransomware binary file to %windir%\system32 and take ownership of it (takeown.exe /F filepath) and reset the ACL permissions. In other cases an Alternate Data Stream (ADS) is used as a means to run the ransomware processes.
- Create and run a service. The service is deleted once the encryption process is completed.

IOC's

*wasted and *wasted_info filenames for encrypted files and the ransom notes

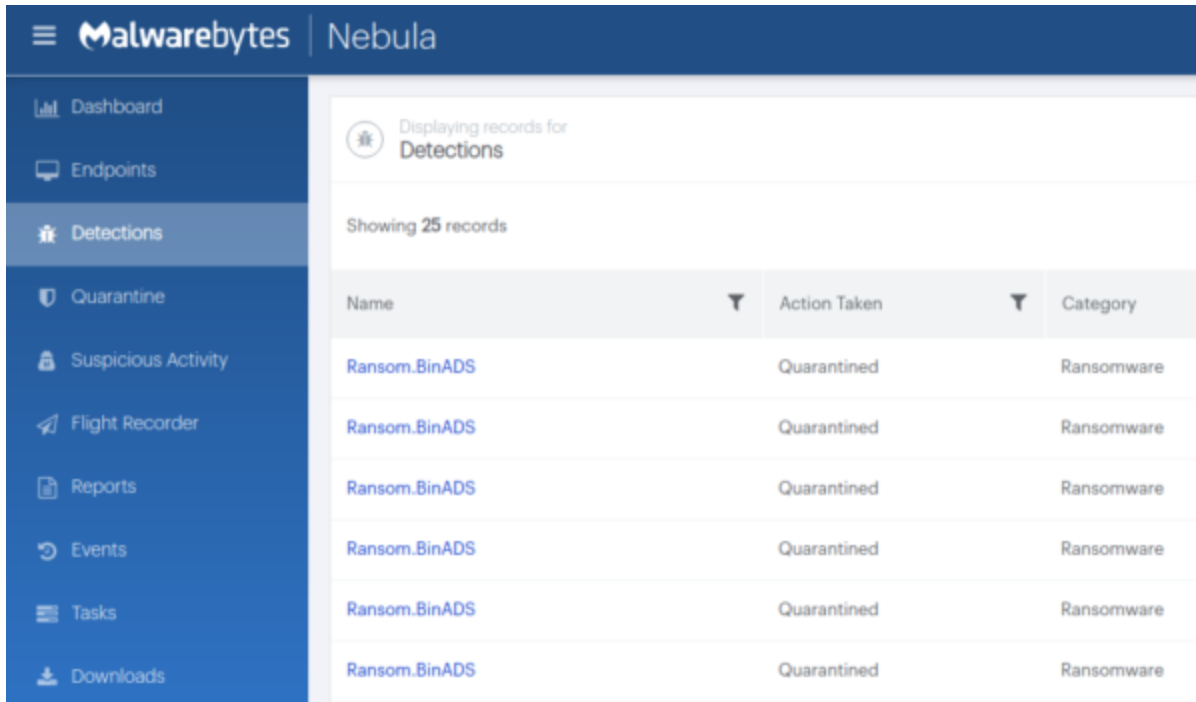
Basic layout of the content of the ransom note:

```
*ORGANIZATION_NAME*
YOUR NETWORK IS ENCRYPTED NOW
USE *EMAIL1* | *EMAIL2* 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]*[end_key]
KEEP IT
```

The email addresses are usually numeric and 5 digits, one at Protonmail and the other at Airmail, but we have also seen Tutanota and Eclipso email addresses.

Malwarebytes detection

Malwarebytes detects WastedLocker ransomware as Ransom.BinADS.



The screenshot shows the Malwarebytes Nebula interface. The left sidebar contains navigation options: Dashboard, Endpoints, Detections (selected), Quarantine, Suspicious Activity, Flight Recorder, Reports, Events, Tasks, and Downloads. The main content area displays 'Displaying records for Detections' and 'Showing 25 records'. A table lists six detection records, all identified as 'Ransom.BinADS' and marked as 'Quarantined'.

Name	Action Taken	Category
Ransom.BinADS	Quarantined	Ransomware
Ransom.BinADS	Quarantined	Ransomware
Ransom.BinADS	Quarantined	Ransomware
Ransom.BinADS	Quarantined	Ransomware
Ransom.BinADS	Quarantined	Ransomware
Ransom.BinADS	Quarantined	Ransomware

Stay safe everyone!