BlackMatter: New Data Exfiltration Tool Used in Attacks

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration

At least one affiliate of the BlackMatter ransomware operation has begun using a custom data exfiltration tool in its attacks. Exmatter, which was discovered by Symantec's Threat Hunter Team, is designed to steal specific file types from a number of selected directories and upload them to an attacker-controlled server prior to deployment of the ransomware itself on the victim's network.

This is the third time a custom data exfiltration tool appears to have been developed by ransomware operators, following the earlier discovery of the Ryuk Stealer tool and StealBit, which is linked to the LockBit ransomware operation.

Exmatter in action

Exmatter is compiled as a .NET executable and obfuscated. When run, it checks its command line arguments for the following strings: "nownd" and "-nownd". If either is found, it attempts to hide its own window by calling the "ShowWindow" API as follows:

```
ShowWindow(Process.GetCurrentProcess().MainWindowHandle, 0);
```

In order to identify files for exfiltration, it will retrieve the drive names of all logical drives on the infected computer and collect all file path names, disregarding anything under the following directories:

- C:\Documents and Settings
- C:\PerfLogs
- C:\Program Files\Windows Defender Advanced Threat Protection\Classification\Configuration
- C:\Program Files\WindowsApps
- C:\ProgramData\Application Data
- C:\ProgramData\Desktop
- C:\ProgramData\Documents
- C:\ProgramData\Microsoft
- C:\ProgramData\Packages
- C:\ProgramData\Start Menu
- C:\ProgramData\Templates
- C:\ProgramData\WindowsHolographicDevices
- C:\Recovery
- C:\System Volume Information
- C:\Users\All Users
- C:\Users\Default
- C:\Users\Public\Documents
- C:\Windows

It will also exclude files of less than 1,024 bytes in size and files with the following attributes:

- FileAttributes.System
- FileAttributes.Temporary
- FileAttributes.Directory

It will only exfiltrate files with the following extensions:

- .doc
- .docx
- .xls
- .xlsx
- .pdf
- .msg
- .png
- .ppt
- .pptx
- .sda
- .sdm
- .sdw
- .csv

It attempts to prioritize files for exfiltration by using LastWriteTime.

Files that match the criteria are then uploaded to a remote SFTP server using the following parameters:

- Host: 165.22.84.147
- Port: 22

Exmatter also includes SOCKS5 configuration, but this is not used:

- Host: 10.26.16.181
- Port: 1080

When it has finished exfiltrating data, Exmatter starts the following process to remove any trace of itself:

- Filename: "powershell.exe"
- Arguments:

  ```
  -WindowStyle Hidden -C $path =
  '[FILEPATH_OF_THE_EXECUTING_SAMPLE]';Get-Process | Where-Object
  {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[]
  65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
  ```

This will attempt to overwrite an initial chunk of the file before deleting it.

Newer variants

Multiple variants of Exmatter have been found, suggesting that the attackers have continued to refine the tool in order to expedite exfiltration of a sufficient volume of high value data in as short a time as possible.

In a second variant, the directory “C:\Program Files\Windows Defender Advanced Threat Protection\Classification\Configuration” has been replaced with “C:\Program Files\Windows Defender Advanced Threat Protection" on the exclusion list. The file types “.xlsm”, and “.zip” were added to the inclusion list.

A third version of note added a WebDav client. The code structure suggests that SFTP remains the first choice protocol, with WebDav acting as a backup. The WebDav client uses the following URL:

https://157.230.28.192/data/

The following file types were also added to the inclusion list:

- .json
- .config
- .ts

- .cs
- .js
- .aspx
- .pst

In addition to this, Exmatter is configured to skip exfiltration for files with names containing any of the following strings:

- OneDriveMedTile
- locale-
- SmallLogo
- VisualElements
- adobe_sign
- Adobe Sign
- core_icons

A fourth variant contained updated SFTP server details:

- Host: 159.89.128.13
- Port: 22

The WebDav client used the following updated URL:

> https://159.89.128.13/data/

Finally, the list of files for inclusion was updated by removing “.png”.

Veteran ransomware operators

BlackMatter is linked to the Coreid cyber crime group, which was previously responsible for the Darkside ransomware. For the past 12 months, it has been one of the most prolific targeted ransomware operators and its tools have been used in a number of ambitious attacks, most notably the May 2021 Darkside attack on Colonial Pipeline that disrupted fuel supplies to the East Coast of the U.S.

Coreid operates under a RaaS model, working with affiliates to conduct ransomware attacks and then taking a share of the profits. Like most ransomware actors, attacks linked to Coreid steal victims’ data and the group then threatens to publish it to further pressure victims into paying the ransom demand. Whether Exmatter is the creation of Coreid itself or one of its affiliates remains to be seen, but its development suggests that data theft and extortion continues to be a core focus of the group.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f3738bcfbd3f832a1

5e355f90b398cbb54829038c6e5d68e8c578405d142bdcc2386cf6161c8d7014

8eded48c166f50be5ac33be4b010b09f911ffc155a3ab76821e4febd369d17ef

b6bc126526e27c98a94aab16989864161db1b3a75f18bd5c72bacbdfccad7bd7

fcaed9faa026a26d00731068e956be39235487f63e0555b71019d16a59ea7e6b

157.230.28.192

159.89.128.13

165.22.84.147