This ransomware strain is trying to disable Windows Defender and Malwarebytes

That is Clop CryptoMix.

That is Clop CryptoMix - a type of ransom malicious code belonging to CryptoMix strain which has been raining all over the world in recent months. To successfully encrypt the victim's data, Clop CryptoMix is ?? currently trying to disable Windows Defender as well as remove the standalone Anti-Ransomware programs of Microsoft Security Essentials and Malwarebytes.

Basically, Clop CryptoMix is ??a variant of CryptoMix Ransomware, uses the .Clop extension and owns a ransom note called CIopReadMe.txt (signature: "Dont Worry C | 0P"). You could call this ransom malicious code Clop.

Try to disable Windows Defender

According to analysis done by renowned security researcher Vitali Kremez, Clop has added the ability to silently execute a special technique, allowing it to disable many types of security software before code. Data of victims, including Windows Defender and some security software of Malwarebytes.

This is essentially a technique that helps combat file encryption detection behavior algorithms as well as blocking security software ransomware.

To disable Windows Defender, Clop will configure various Registry values ??to disable behavior monitoring, real-time protection, malicious code uploads to Microsoft, Tamper Protection, cloud security and detect anti-spyware software . of this program.

The good news is that if you have Tamper Protection turned on in Windows 10, these settings will be reset to their default settings and Windows Defender will still function normally without being disabled, and vice versa.

In addition to Windows Defender, Clop is also targeting older computers by uninstalling Microsoft Security Essentials. The fact that CryptoMix is ??run by admin privileges from the attackers, so it is possible to completely remove the software without any problems.

Try to uninstall Malwarebytes Anti-Ransomware

Security team MalwareHunterteam has discovered that besides Windows Defender, Clop is similarly targeting the standalone Malwarebytes Anti-Ransomware program.

When executed, the malicious code will attempt to disable Malwarebytes Anti-Ransomware programs with the following command:

```
C: Program FilesMalwareBytesAnti-Ransomwareunins000.exe / verysilent / suppres
```

On the other hand, CryptoMix is ??usually installed via Remote Desktop or penetrated the network, so targeting products that old enterprise workstations may be using allows this ransomware software to self because it works without any barriers to encryption of the entire network.

Neither Microsoft nor Malwarebytes have commented on the findings.