Clop Ransomware Now Kills Windows 10 Apps and 3rd Party Tools

By Lawrence Abrams

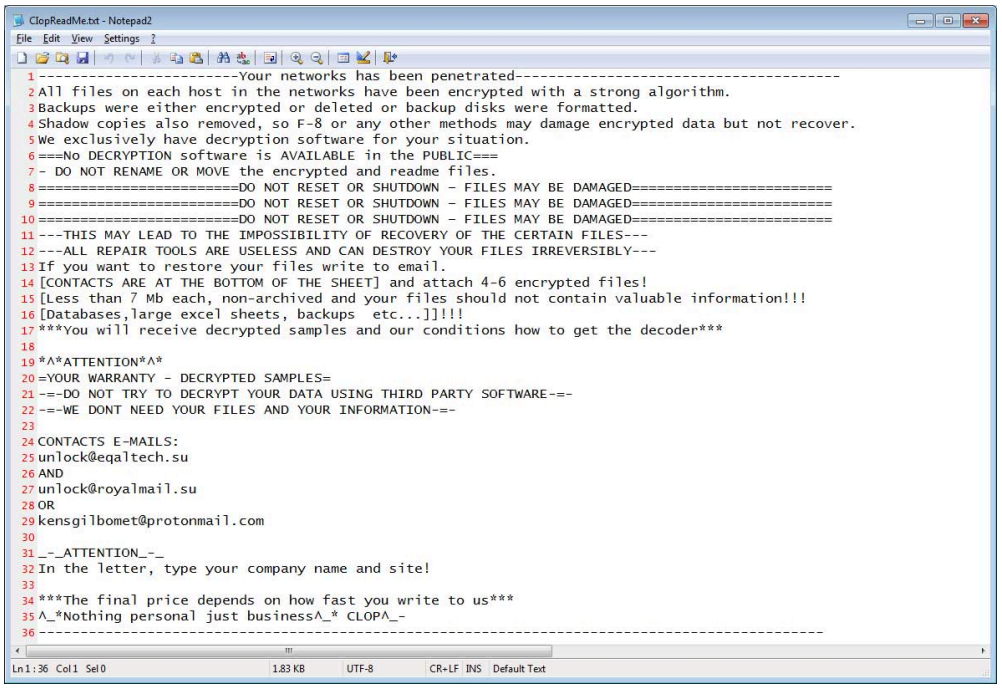
Published: 2020-01-03 · Archived: 2026-04-02 11:09:21 UTC

The Clop Ransomware continues to evolve with a new and integrated process killer that targets some interesting processes belonging to Windows 10 apps, text editors, programming IDEs and languages, and office applications.

When the Clop Ransomware started circulating in February 2019, it was just your normal garden variety CryptoMix ransomware variant with the same features we have been seeing in this family since 2017.

In March 2019, though, the Clop Ransomware suddenly changed and began disabling services for Microsoft Exchange, Microsoft SQL Server, MySQL, BackupExec, and other enterprise software. The ransom note had also changed to indicate that the attackers were targeting an entire network rather than individual PCs.


Outlook
f5
Outlook



Clop Ransom Note

It was determined at that time, that a threat actor group known as TA505 had adopted the Clop Ransomware as their final payload of choice after compromising a network, similar to how Ryuk, BitPaymer, and DoppelPaymer were being used.

This adoption by the threat actors has most likely fueled the ransomware's development as the actors change it to fit their needs when performing network-wide encryption.

Development continued in November 2019, when a new variant was released that attempted to disable Windows Defender running on local computers so that it would not be detected by future signature updates.

These changes also coincided with the threat actors continued targeting of companies in the Netherlands and France.

Just last month, Maastricht University (UM) in the Netherlands was infected by the Clop Ransomware.

Clop now terminates 663 processes

In late December 2019 a new Clop variant was discovered by MalwareHunterTeam and reverse engineered by Vitali Kremez that add improves their process termination feature; Clop now terminates 663 Windows processes before encrypting files.

It is not uncommon for ransomware to terminate processes before encrypting files as the attackers want to disable security software and do not want any files to be open as it could prevent them from being encrypted.

This new variant takes it a step further by terminating a total of 663 processes, which include new Windows 10 apps, popular text editors, debuggers, programming languages, terminal programs, and programming IDE software.

Some of the more interesting processes that are terminated include the Android Debug Bridge, Notepad++, Everything, Tomcat, SnagIt, Bash, Visual Studio, Microsoft Office applications, programming languages such as Python and Ruby, the SecureCRT terminal application, the Windows calculator, and even the new Windows 10 Your Phone app.

```
 ACROBAT.EXE
ADB.EXE
CODE.EXE
CALCULATOR.EXE
CREATIVE CLOUD.EXE
ECLIPSE.EXE
```

```
EVERYTHING.EXE
JENKINS.EXE
MEMCACHED.EXE
MICROSOFTEDGE.EXE
NOTEPAD++.EXE
POWERPNT.EXE
PYTHON.EXE
QEMU-GA.EXE
RUBY.EXE
SECURECRT.EXE
SKYPEAPP.EXE
SNAGIT32.EXE
TOMCAT7.EXE
UEDIT32.EXE
WINRAR.EXE
WINWORD.EXE
YOURPHONE.EXE
```

It is not known why some of these processes are terminated, especially ones like Calculator, Snagit, and SecureCRT, but its possible they want to encrypt configuration files used by some of these tools.

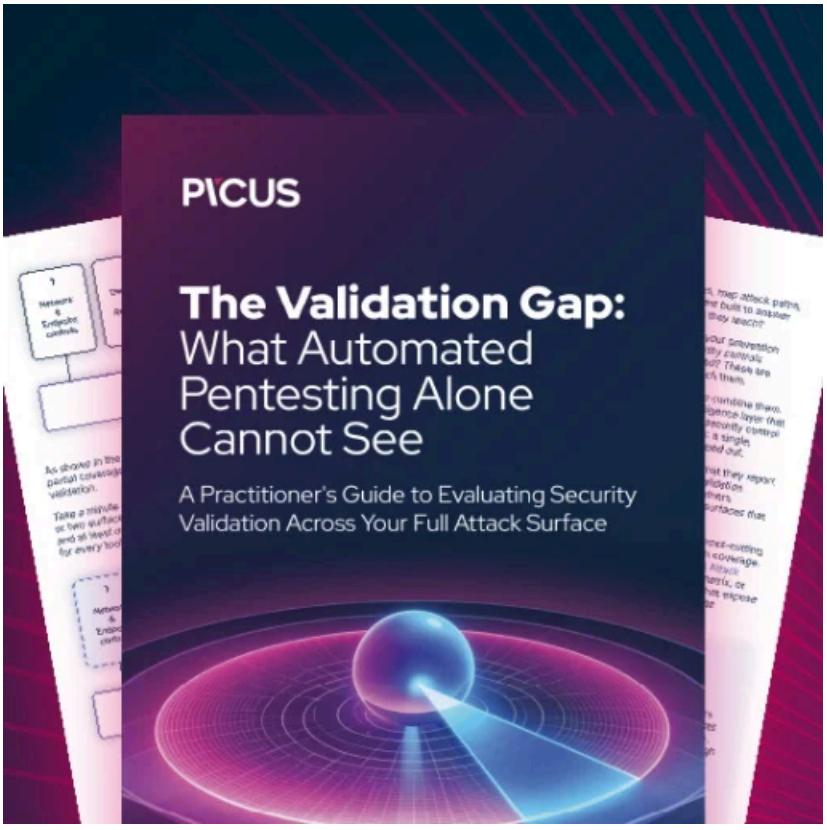
A full list of the terminated processes can be found in Kremez's GitHub repository.

In the past, the process termination functionality was performed by a Windows batch file. By embedding this functionality into the main executable, it further signifies active development by the group.

"This change signifies that the ransomware group decided to include the "process killer" in the main bot making it a more universal Swiss-army approach rather than relying on their external libraries like "av_block" for this purpose," Kremez told BleepingComputer in a conversation.

In addition to the new and large list of targeted processes, this Clop Ransomware variant also utilizes a new .Cl0p extension, rather than the .CIop or .Clop extensions used in previous versions.

As Clop continues to infect organizations, and reap large ransoms for doing so, we can expect to see its development to continue as the actors evolve their tactics.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-now-kills-windows-10-apps-and-3rd-party-tools/