Malware

New LockFile ransomware gang weaponizes ProxyShell and PetitPotam attacks

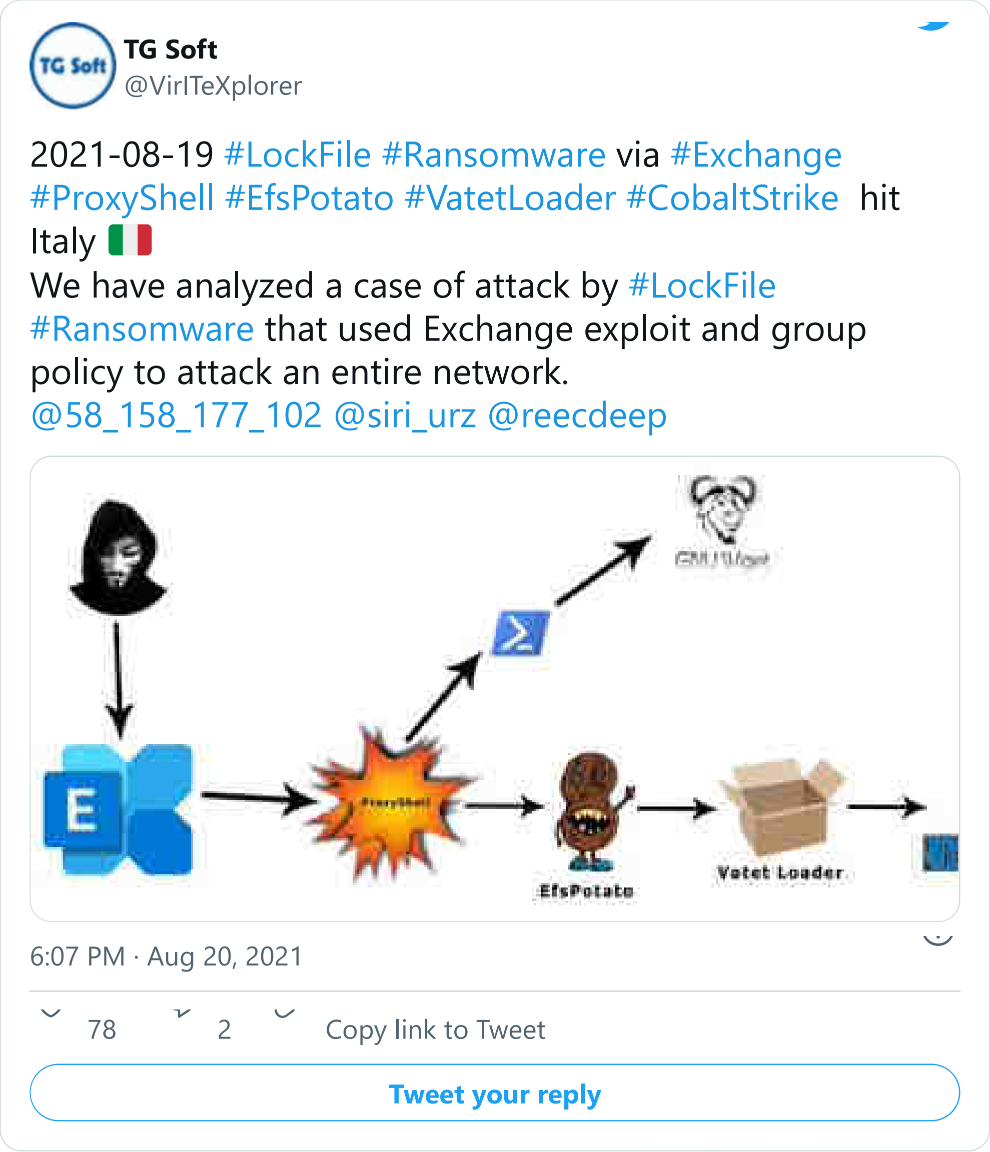
Image: The Record

A new ransomware group has weaponized two recently disclosed vulnerabilities in order to improve their chances at breaching, taking over, and encrypting corporate networks.

Named **LockFile**, this new ransomware gang has been seen exploiting a vulnerability known as ProxyShell to gain access to Microsoft Exchange email servers, from where it pivots to companies' internal networks, according to reports from security firm TG Soft and security researcher Kevin Beaumont.

Once inside, LockFile operators abuse an attack method known as PetitPotam to take over a company's Windows domain controller and then deploy their file-encrypting payloads to connected workstations, according to a report published on Friday by security firm Symantec.

Details about the PetitPotam attack and the ProxyShell vulnerability have been disclosed at the end of July and early August, respectively, showing once again that cybercrime gangs are quite quick to weaponize exploits when they enter the public domain.



TG Soft
@VirITeXplorer

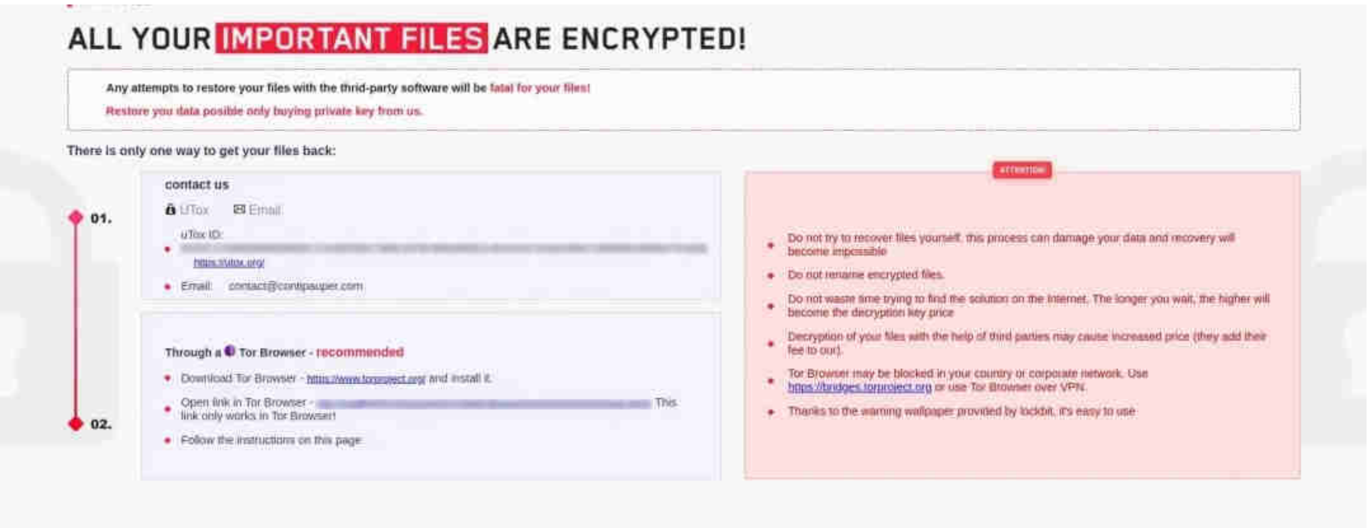
2021-08-19 #LockFile #Ransomware via #Exchange #ProxyShell #EfsPotato #VatetLoader #CobaltStrike hit Italy 🇮🇹
We have analyzed a case of attack by #LockFile #Ransomware that used Exchange exploit and group policy to attack an entire network.
@58_158_177_102 @siri_urz @reecdeep

6:07 PM · Aug 20, 2021

Symantec said the group has already hit at least ten organizations, with most of its victims based in the US and Asia.

“The LockFile ransomware was first observed on the network of a US financial organization on July 20, 2021, with its latest activity seen as recently as August 20,” the company said last week.

Currently, details about this ransomware operation are still scarce. What is known is that LockFile is trying to mimic the visual style of the ransom notes used by LockBit, a more well-known ransomware gang that recently has seen a spike in use in the criminal underworld.



ALL YOUR IMPORTANT FILES ARE ENCRYPTED!

Any attempts to restore your files with the thrid-party software will be fatal for your files!

Restore you data posible only buying private key from us.

There is only one way to get your files back:

01.

contact us

UTox Email

- uTox ID: [redacted] https://utox.org/
- Email: contact@contipauper.com

02.

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it.
- Open link in Tor Browser - [redacted] This link only works in Tor Browser!
- Follow the instructions on this page

ATTENTION

- Do not try to recover files yourself. this process can damage your data and recovery will become impossible
- Do not rename encrypted files.
- Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
- Thanks to the warning wallpaper provided by lockbit. it's easy to use

Image: Symantec

To prevent the LockFile gang from gaining access to their systems, companies are advised to apply patches for the PetitPotam and ProxyShell vulnerabilities.

PetitPotam patches and mitigations are detailed here.

ProxyShell security patches have shipped with May and July Windows security updates (CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523).

Catalin Cimpanu

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

PREVIOUS

« Almost 2,000 Exchange servers hacked using ProxyShell exploit

SHARE

PUBLISHED BY

Catalin Cimpanu

TAGS:

LockBit / LockFile / malware / Microsoft Exchange / PetitPotam / ProxyShell / RaaS / Ransomware