Hive Pro

THREAT ADVISORY

ProxyShell and PetitPotam exploits weaponized by LockFile Ransomware Group	TA202131
Threat Level RED	**Publish Date –** Aug 24, 2021

LockFile, a new ransomware gang, has been active since last week. LockFile began by using a publicly disclosed PetitPotam exploit (CVE-2021-36942) to compromise Windows Domain Controllers earlier this week. Using ProxyShell vulnerabilities(CVE-2021-34473, CVE-2021-34523 and CVE-2021-31207), they've now infiltrated many Microsoft Exchange Servers . The origins of this gang are most likely China. This gang used a similar ransomware note as of LokiBot and is been linked to Conti ransomware due to the email id provided(contact@contipauper[.]com). HivePro Threat Research team advises everyone to patch the vulnerabilities to prevent an attack.

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name
CVE-2021-34473	Microsoft Exchange Server 2013 CU23, 2016 CU19, 2016 CU20, 2019 CU8, 2019 CU9	cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu19:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu20:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu8:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu9:*:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-34523			Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2021-36942			Windows LSA Spoofing Vulnerability
CVE-2021-31207			Microsoft Exchange Server Security Feature Bypass Vulnerability

Actor Details

Name	Target Locations	Target sectors
LockFile Ransomware	United States of America and Asia	manufacturing, financial services, engineering, legal, business services, and travel and tourism sectors

Hive Pro

THREAT ADVISORY

Indicators of Compromise (IoCs)

Type	Value
IP Address	209.14.0.234
SHA-2 Hash	ed834722111782b2931e36cfa51b38852c813e3d7a4d16717f59c1d037b62291 cafe54e85c539671c94abdeb4b8adbef3bde8655006003088760d04a86b5f915 36e8bb8719a619b78862907fd49445750371f40945fefd55a9862465dc2930f9 5a08ecb2fad5d5c701b4ec42bd0fab7b7b4616673b2d8fbd76557203c5340a0f 1091643890918175dc751538043ea0743618ec7a5a98018785549700365 24b75 2a23fac4cfa697cc738d633ec00f3fbe93ba22d2498f14dea08983026fdf128a 7bcb25854ea2e5f0b8cfca7066a13bc8af8e7bac6693dea1cdad5ef193b052fd c020d16902bd5405d57ee4973eb25797087086e4f8079fac0fd8420c716ad153 a926fe9fc32e645bdde9656470c7cd005b21590cda222f72daf854de9ffc4fe0 368756bbcaba9563e1eef2ed2ce59046fb8e69fb305d50a6232b62690d33f690 d030d11482380ebf95aea030f308ac0e1cd091c673c7846c61c625bdf11e5c3a a0066b855dc93cf88f29158c9ffbbdca886a5d6642cbcb9e71e5c759ffe147f8

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows
https://www.bleepingcomputer.com/news/security/lockfile-ransomware-uses-petitpotam-attack-to-hijack-windows-domains/