Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

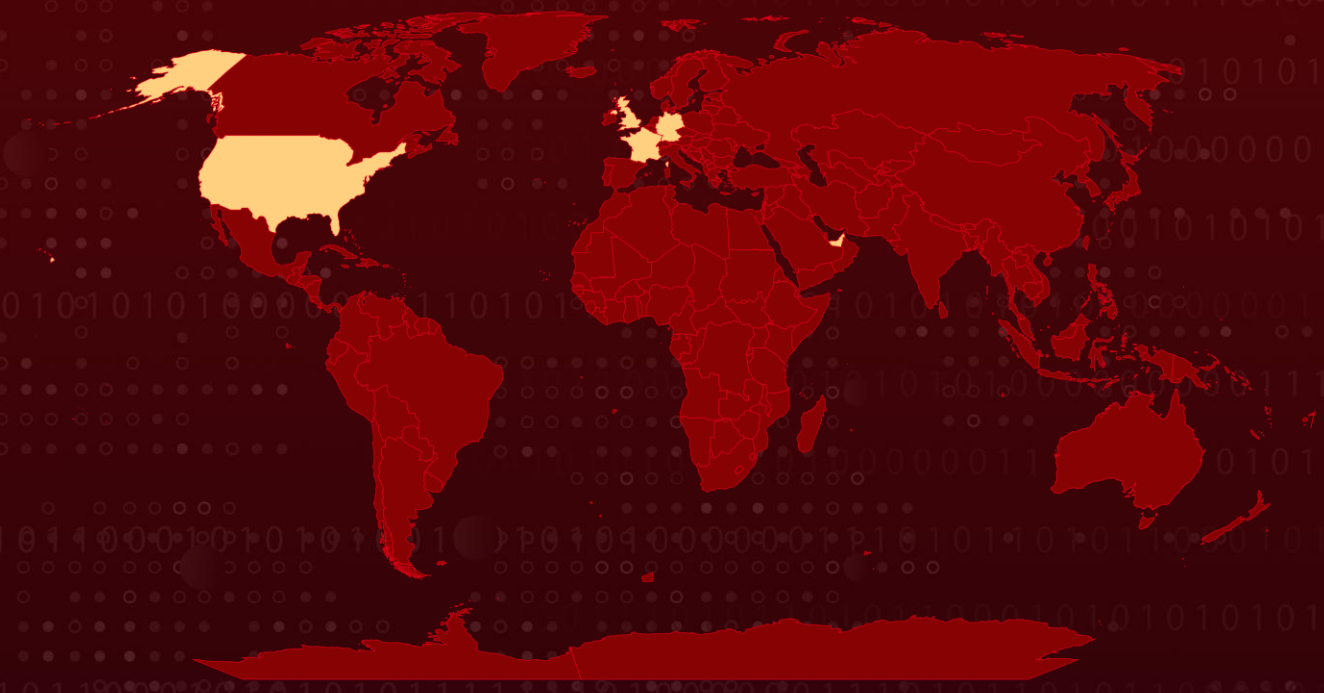
Linux Variant of Cl0p Ransomware Discovered with Flawed Encryption Algorithm

Date of Publication	Admiralty Code	TA Number
February 8, 2023	A1	TA2023068

Summary

First appeared: December 26, 2022
Attack Region: United Kingdom, United States, France, Germany, United Arab Emirates.
Attack Sector: Utilities, Internet Software & Services, Construction, Engineering, Retail, Professional Services, Communications, Electrical, Food Products
Attack: A new variant of the Cl0p ransomware for Linux has been discovered. The executable file in ELF format has a flawed encryption algorithm, which allows for the decryption of the locked files without requiring a ransom payment.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The first-ever ELF variant of Cl0p (also known as Clop) ransomware has been detected in the wild. However, the ELF executable contains a flawed encryption algorithm, allowing for the decryption of locked files without paying the ransom. The Linux version is designed to encrypt specific folders and file types, but it includes a hard-coded master key that can be utilized to retrieve the original files without paying the adversary.

#2 The ransomware first invokes the fork to initiate a new process and terminates the parent process. The child process then sets its file mode creation mask to any permission by calling umask. It starts a session and assigns a process group ID by invoking setsid. The ransomware then tries to access the root by changing the working directory. After specifying the permissions, it will encrypt other directories.

#3 The Linux version of Clop ransomware leaves a ransom note with a .txt extension on infected devices, which is slightly different from the Windows .rtf ransom note, although both use the same email addresses for victims to contact the attackers.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0040** Impact	**T1497** Virtualization/Sandbox Evasion	**T1497.003** Time Based Evasion
T1140 Deobfuscate/Decode Files or Information	**T1027** Obfuscated Files or Information	**T1573** Encrypted Channel	**T1059** Command and Scripting Interpreter
T1083 File and Directory Discovery	**T1560** Archive Collected Data	**T1106** Native API	**T1553** Subvert Trust Controls
T1471 Data Encrypted for Impact	**T1543** Create or Modify System Process	**T1543.002** Systemd Service	**T1070** Indicator Removal
T1070.004 File Deletion	**T1027.005** Indicator Removal from Tools	**T1082** System Information Discovery	**T1518** Software Discovery
T1518.001 Security Software Discovery	**T1071** Application Layer Protocol	**T1090** Proxy	**T1059.003** Windows Command Shell
T1486 Data Encrypted for Impact	**T1027.002** Software Packing	**T1057** Process Discovery	**T1489** Service Stop

Indicators of Compromise (IOCs)

TYPE	VALUE
Emails	unlock[@]support-mult.com unlock[@]rsv-box.com
URLs	hxxp[:]//santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad[.]onion hxxp[:]//6v4q5w7di74grj2vtmikzgx2tnq5eagyg2cubpcnqrvvee2ijpmprzqd[.]onion

TYPE	VALUE
SHA1	46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5 40b7b386c2c6944a6571c6dcfb23aaae026e8e82 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d a1a628cca993f9455d22ca2c248ddca7e743683e a6e940b1bd92864b742fbd5ed9b2ef763d788ea7 ac71b646b0237b487c08478736b58f208a98eebf ba5c5b5cbd6abdf64131722240703fb585ee8b56 77ea0fd635a37194efc1f3e0f5012a4704992b0e

Recent Breaches

https://www.ftsumnerk12.com/
https://www.ferran-services.com/
https://alexim.com/
https://capcarpet.com/
https://www.orbitelectric.com/
https://enssecurity.com/
https://drc-law.com/
https://www.applexus.com/
https://thenoc.net/
https://www.zisserfamilylaw.com/
https://www.fair-rite.com/
https://www.latournerie-wolfrom.com/en/home/
https://www.thameswater.co.uk/
https://www.atapcoproperties.com/
https://perbit.com/
http://afjconsulting.net/
https://driveandshine.com/
http://marcelsolution.com/
https://www.spinneys.com/en-ae/
http://orderexpress.com/
https://jbinstantlawn.net/
https://www.jdavidtaxlaw.com/

References

https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/

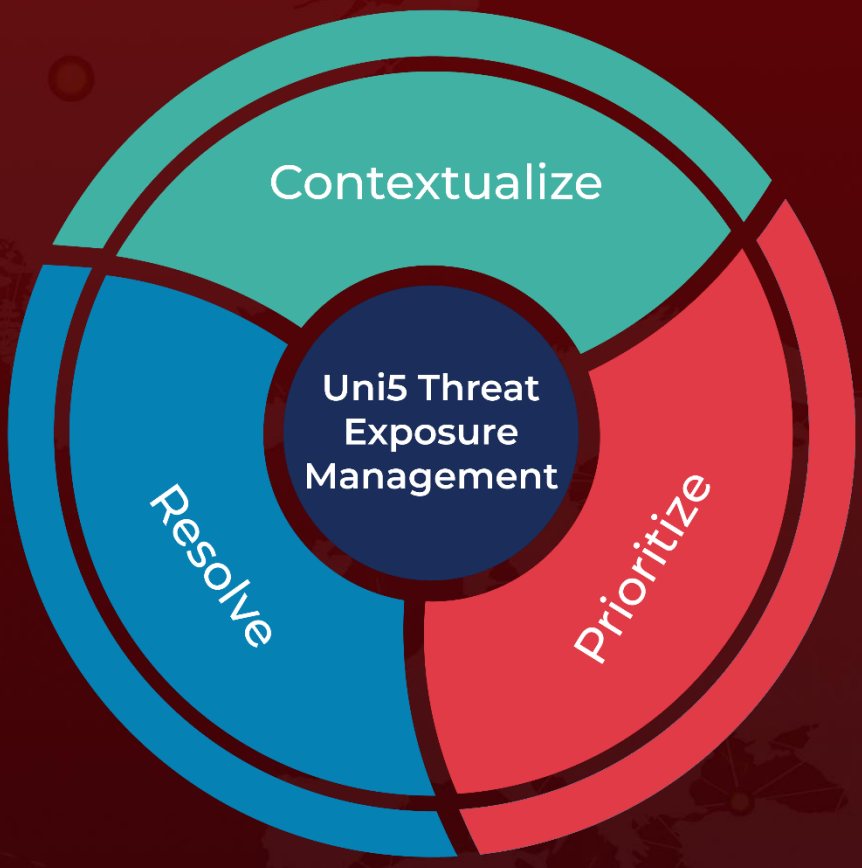
https://www.hivepro.com/truebot-exploits-vulnerability-in-netwrix-to-deploy-clop-ransomware/

https://attack.mitre.org/software/S0611/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 8, 2023 • 1:11 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com