Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

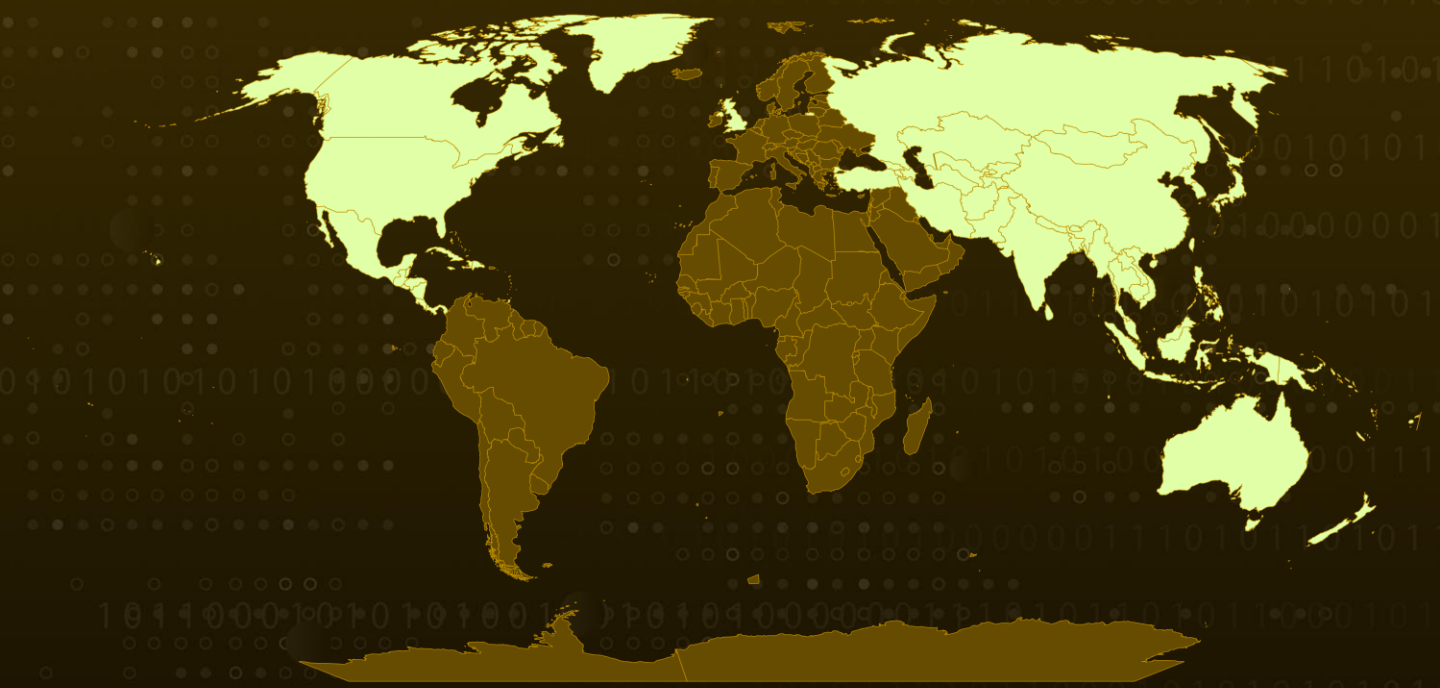
Deceptive Discord Campaign Targets Government Entities with PureCrypter Malware

Date of Publication	Admiralty Code	TA Number
February 27, 2023	A1	TA2023104

Summary

First appeared: March 2021
Attack Region: Asia-Pacific and North American regions.
Attack Sector: Government
Attack: Government entities in the Asia-Pacific and North American regions have been targeted by a threat actor using the PureCrypter malware downloader. This particular malware has been used to distribute various strains of ransomware and information stealers. The PureCrypter campaign leverages a compromised non-profit organization's domain as a Command and Control (C2) to deliver a secondary payload.

Attack Regions



Attack Details

#1

An unidentified threat actor has targeted government institutions with a deceptive threat campaign that is being disseminated on Discord. The campaign employs the PureCrypter downloader and uses the domain of a hacked non-profit organization as a Command and Control (C2) to deliver a secondary payload. The campaign has been identified to spread a variety of malware, including Redline Stealer, AgentTesla, Eternity, Blackmoon, and Philadelphia Ransomware.

#2

PureCrypter, a sophisticated downloader, has been utilized in recent campaigns to download Remote Access Trojans (RATs) and Infostealers. Furthermore, PureCrypter is downloading a secondary malware known as AgentTesla. AgentTesla is a robust backdoor built on .NET that can harvest stored passwords from various browsers, and keyloggers, and capture images.

#3

The attack commences with an email that contains a Discord app URL that directs to a password-protected ZIP archive containing a PureCrypter sample. Once executed, the next-stage payload is delivered from a C2 server, which is the compromised server of a non-profit organization in this case. Upon launching, it establishes a connection to a Pakistan-based FTP server used to receive the stolen data. The downloaded binary is packed to avoid initial detection and includes the AgentTesla payload, which is encrypted in the resource section using the DES Algorithm.

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

TA0002 Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**T1047** Windows Management Instrumentation
T1055 Process Injection	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1497** Virtualization/Sandbox Evasion
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1036** Masquerading	**T1003** OS Credential Dumping
T1082 System Information Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1010** Application Window Discovery
T1057 Process Discovery	**T1005** Data from Local System	**T1095** Non-Application Layer Protocol	**T1071** Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	be18d4fc15b51daedc3165112dad779e17389793fe0515d62bbcf00def2c3c2d,5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2cd80e99,a7c006a79a6ded6b1cb39a71183123dcaaaa21ea2684a8f199f27e16fcb30e8e,5d649c5aa230376f1a08074aee91129b8031606856e9b4b6c6d0387f35f6629d,f950d207d33507345beeb3605c4e0adfa6b274e67f59db10bd08b91c96e8f5ad,397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3,7a5b8b448e7d4fa5edc94dcb66b1493adad87b62291be4ddcbd61fb4f25346a8,efc0b3bfcec19ef704697bf0c4fd4f1cfb091dbfee9c7bf456fac02bcffcfedf,c846e7bbbc1f65452bdca87523edf0fd1a58cbd9a45e622e29d480d8d80ac331
MD5	967f9bc90202925e1f941c8ea1db2c94 bcf031ab2b43dc382b365ba3df9f09bc f34d5f2d4577ed6d9ceec516c1f5a744 61259b55b8912888e90f516ca08dc514 14e4bfe2b41a8cf4b3ab724400629214 f1c29ba01377c35e6f920f0aa626eaf5 5420dcbae4f1fba8afe85cb03dcd9bfc 18e9cd6b282d626e47c2074783a2fa78 2499343e00b0855882284e37bf0fa327

TYPE	VALUE
MD5	0d8b1ad53fddacf2221409c1c1f3fd70 2499343e00b0855882284e37bf0fa327 0d8b1ad53fddacf2221409c1c1f3fd70 17f512e1a9f5e35ce5761dba6ccb09cb b5c60625612fe650be3dcbe558db1bbc a478540cda34b75688c4c6da4babf973 765f09987f0ea9a3797c82a1c3fced46 bbd003bc5c9d50211645b028833bbeb2 71b4db69df677a2acd60896e11237146 f4eebe921b734d563e539752be05931d b4fd2d06ac3ea18077848c9e96a25142 1d3c8ca9c0d2d70c656f41f0ac0fe818 785bfaa6322450f1c7fe7f0bf260772d 2fa290d07b56bde282073b955eae573e d70bb6e2f03e5f456103b9d6e2dc2ee7 0ede257a56a6b1fbd2b1405568b44015 fdd4cd11d278dab26c2c8551e006c4ed dbcaa05d5ca47ff8c893f47ad9131b29 c9ca95c2a07339edb13784c72f876a60 c3b90a10922eef6d635c6c786f29a5d0 8ef7d7ec24fb7f6b994006e9f339d9af f1c29ba01377c35e6f920f0aa626eaf5 fa4ffa1f263f5fc67309569975611640 754920678bc60dabeb7c96bfb88273de 2964ce62d3c776ba7cb68a48d6afb06e 8503b56d9585b8c9e6333bb22c610b54 eaaf20fdc4a07418b0c8e85a2e3c9b27 b6c849fcdcda6c6d8367f159047d26c4 de94d596cac180d348a4acdeeaaa9439 3f92847d032f4986026992893acf271e ae158d61bed131bcfd7d6cecdccde79b
URLs	hxxps[://]purecoder.sellix[.]io/. hxxps[:]//cdn[.]discordapp.com/attachments/1006638283645784218/1048923462128914512/Private_file__dont_share[.]zip
Domains	purecoder[.]sellix[.]io,ftp[.]mgcpakistan[.]com,cents-ability[.]org
Email	ddd@mgcpakistan[.]com
Registry key	HKLM\Software\Microsoft\Fusion\LoggingLevel

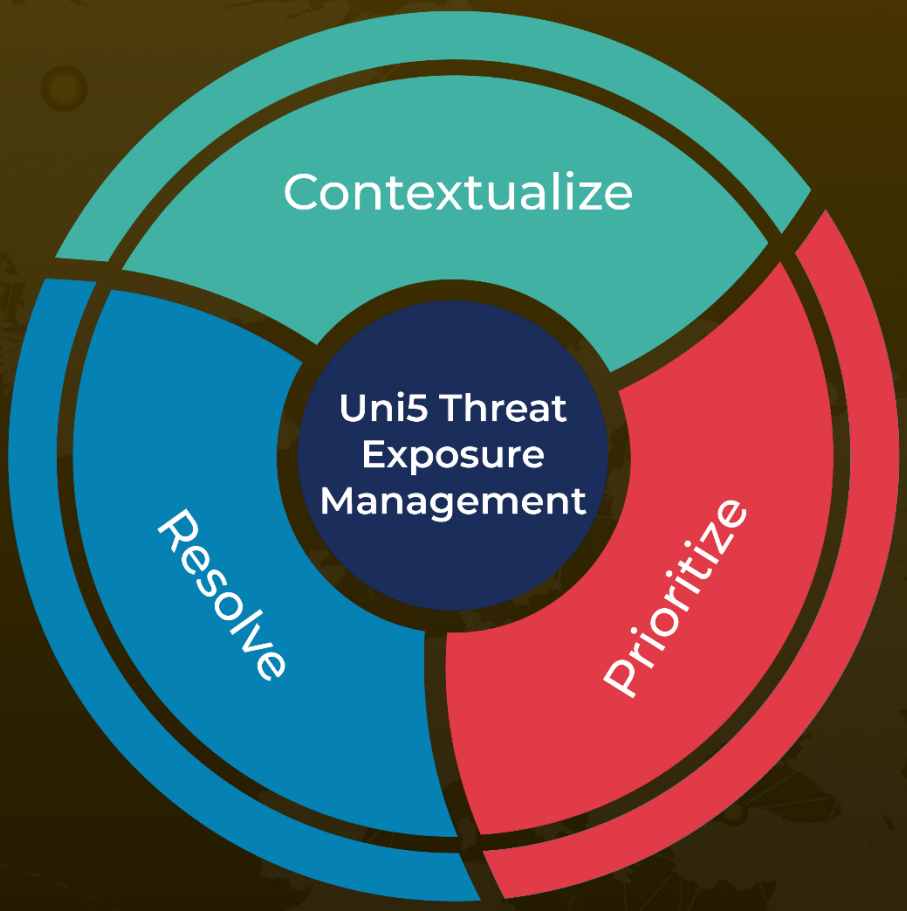
References

https://www.menlosecurity.com/blog/purecrypter-targets-government-entities-through-discord/

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 27, 2023 • 1:22 AM

More at www.hivepro.com