Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

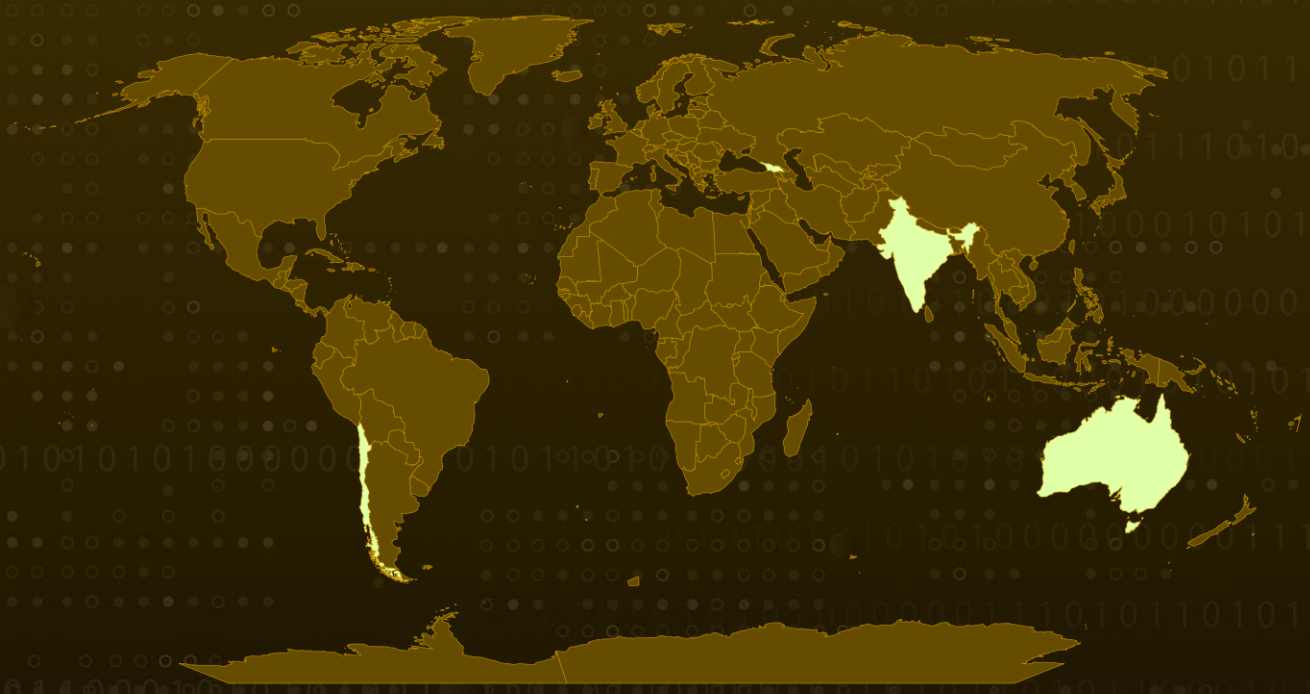
A new strain of Punisher ransomware

Date of Publication	Admiralty Code	TA Number
November 29, 2022	A1	TA2022274

Summary

First appeared: 2018
Attack Region: India, Singapore, Australia, Georgia, Chile
Attack: Encrypts files and demands a ransom of USD 1000 in bitcoin to decrypt them.

Attack Regions



Attack Details

#1 A new variant of the Punisher ransomware is spreading via phishing website that delivers ransomware disguised as a COVID tracking application. Punisher Encryptor is a .NET binary that runs on Windows operating systems.

#2 This binary's compilation time is changed to remain concealed during incident response activities, known as Timestomping. Following the execution, the ransomware rests for five seconds before translating the bytes into Base64 encoded format and sending them to the C&C server.

#3 The MD5 hash is utilized as the final key by the ransomware, which encrypts files using the AES-128 technique and changes the extension of the encrypted files to ".punisher." After infecting a machine, ransomware attaches ransom notes and starts a timer that will also increase the ransom amount after a certain period of time.

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	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1204 User Execution
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1070 Indicator Removal	T1070.006 Timestomp
T1497 Virtualization/Sandbox Evasion	T1497.003 Time Based Evasion	T1087 Account Discovery	T1082 System Information Discovery
T1083 File and Directory Discovery	T1486 Data Encrypted for Impact	T1071 Application Layer Protocol	T1020 Automated Exfiltration

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c267ca8be1871263937a5e433a49342c df3a831a805ada51ce56e32a46a07b51
SHA1	f10f8a99b610db68c2caca017eeb9cd046acea64 7c235d83e6c95a6a7d587d6d3ec99262d52c0fb4
SHA256	79e4ecb131813bd897e9df2f75c32da92ffc603a5a74acb987c90088080774e4, dfc3e3eed6f6bba5e11fb88d06b22d0100188b1776b68b7207e0a4cac09ffa1a
URLs	hxxp[:]//20.100.168[.]3[:]1974/handshake[.]php hxxp[:]//20.100.168[.]3[:]1974/alertmsg[.]zip

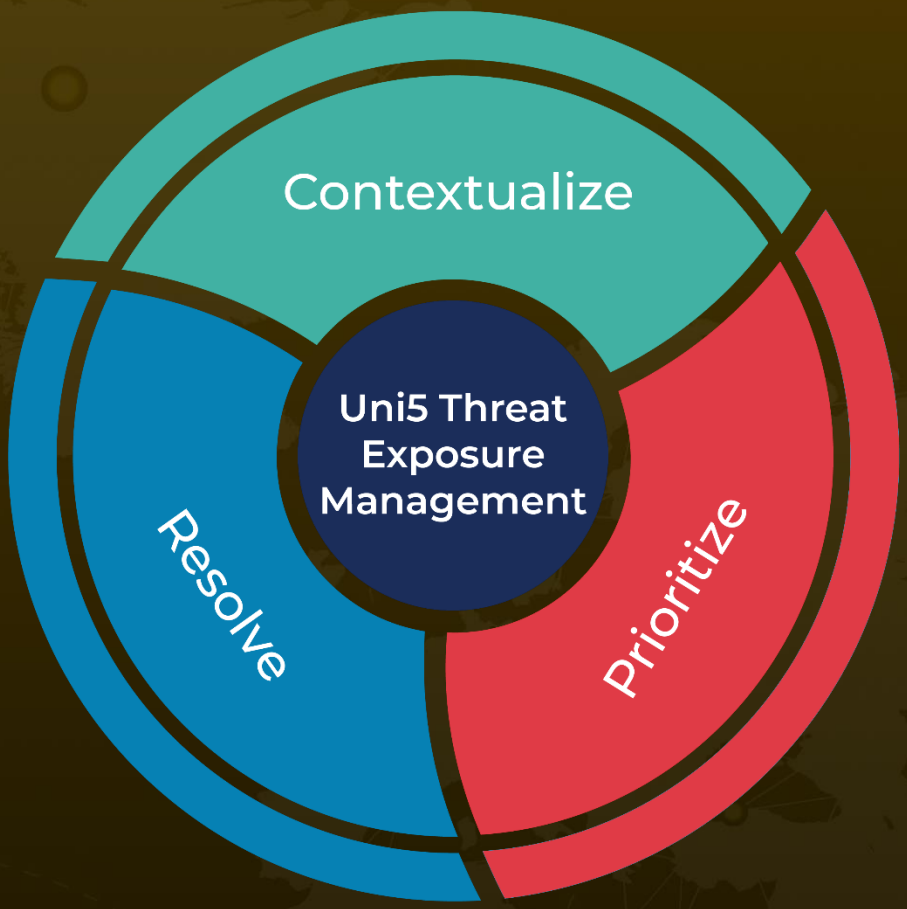
References

https://blog.cyble.com/2022/11/25/punisher-ransomware-spreading-through-fake-covid-site/

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

November 29, 2022 . 3:36 AM

More at www.hivepro.com