Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

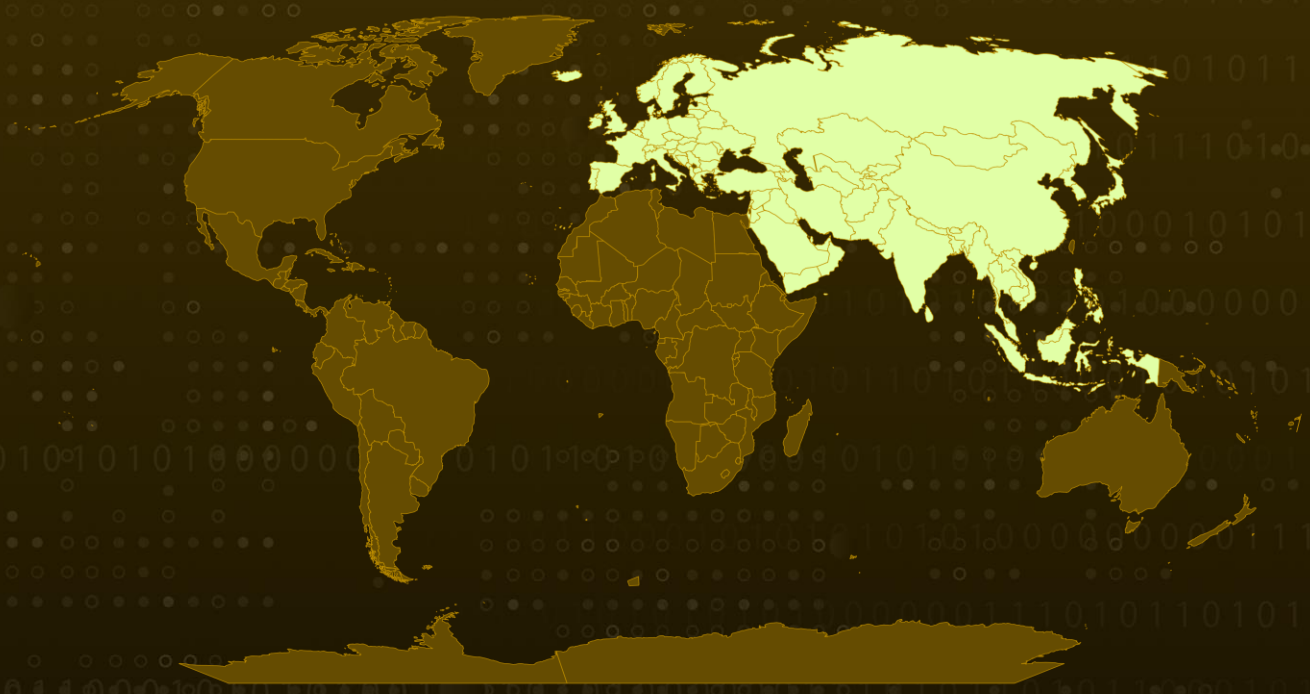
Mallox Ransomware is Ramping up its Operation

Date of Publication	Admiralty Code	TA Number
December 15, 2022	A1	TA2022300

Summary

First appeared: September 2022
Attack Region: Asia and Europe
Attack: Loss of vital data, damage to the organization's reputation, and disruption in business operations.

Attack Regions



Attack Details

#1 Mallox ransomware strains have been spotted in the wild, indicating that the ransomware is operational, propagating rapidly, and infecting entities. An unknown .NET-based loader distributes these Mallox ransomware samples. The loader then downloads and encrypts data on the victim's device with Mallox ransomware from a remote source.

#2 The loader downloads the encrypted malicious content upon execution. The malicious payload is encrypted with the AES encryption algorithm and the hardcoded key "Cwgoawrnxz" in the loader's binary. The loader now decrypts the ransomware DLL file and executes it to carry out ransomware operations.

#3 To make malware reversing more complex, the DLL file is further obfuscated using an IntelliLock obfuscator. Prior to encrypting the files, the ransomware sends system data to the command-and-control (C&C) server. The ransomware then encrypts the files, appends the file extension ".Mallox," and leaves a ransom note in the folders.

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	TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1204 User Execution	T1140 Deobfuscate/Decode Files or Information
T1562 Impair Defenses	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	2456c01f5348e5c08f7e818d51862c1a b739be28cb9a30868112d4786bc11d37 86344d7e6e5b371717313032632cbbe1 688e0b37794395cfecaf9cc519e3c26a 6080b540d975b7a4f66cd54ee83ed600 2ffae162e07ba8debdf25694e8fd8325 cacbed12b83529ebb99b0297d52b0749 da3f02b82e982f5ce5a71d769a067f3b 38454291f7b871d71a512b5dd5100d9e 7be2a76577f6ee05ec08c77c41cd9dd4 6e542eda455e8c8600df96874c8deceb
SHA1	625be3e4dbfb0bd35c9cda216a9bca7232dbec07 296e19773f6fb7190d914ac556abe0125e5d7aa5 3921694be80b2fd5d8007c8155bee018c32fecbb d215d4166dfa07be393459c99067319036eb80ba 62324b38a5a5a2533f3bd401d7afd1c6c4235b08 a1289c3e585e091a7c8f89869a76e40f7e3880fd db6d67f55bce0425baef2348e70f1478d022820e e165cac5ab2b2312f7ed8569c69a75bae48b8316 9e9c04f00822aacaa15d0bcc4749f8e6920d4550 f3cfca7a2160559aa62b4cf42cd15870a4abcae7 670530d36967c5927955d31052dff165a187c1f2

TYPE	VALUE
SHA256	34da973f1d154672b245f7a13e6268b4ffc88dea1ca608206b32759ec5be040c b3ccec8ca26bc3b6597ddb0424a455eb7809e7608f5d62f6c7f5d757d4d32253 b64606198c158f79287b215343d286adf959e89acb054f8f3db706f3c06f48aa 77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5 89c9c14af6ab4f3f93705325dbc32bde6c232d26d22e8f835db24efc18007ea4 d691f44b587c6ed47c2d57b2bf99323877821a318cb0d5aa9899c40a44e81ef3 58726aac2652bedfe47b7e1c73ba39d028e2e6ad188f4ed735d614097be4a23b 7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48 45391bfbb06263f421ac739e1e4b438fb99a0757dcecc68de79b2dbe02c1641e 87a923319c6ea74a9cef5ed7528afdbd4a05e7600ce7f4359e5990ff8769a2ff d755cd96077cebbed84a86e69d1fd84b95e3e5763abc8ac8ec0a7f1df30e9585
URLs	hxxp://80[.]66[.]75[.]98/Chseiyk[.]jpeg hxxp://193[.]106[.]191[.]141/QWEwqdsvsf/ap[.]php

Recent Breaches

http://en.canny-elevator.com/

https://www.ctlp.bo/

https://ctoscredit.com.my/

https://www.aero-tech.co.uk/

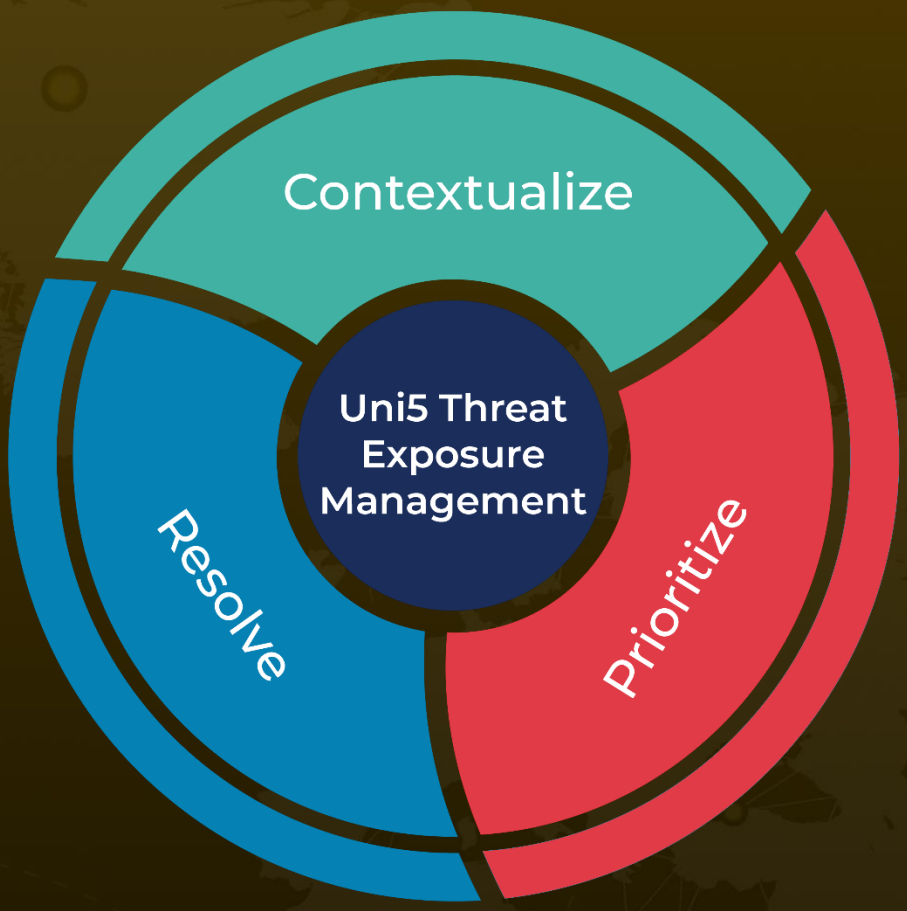
References

https://blog.cyble.com/2022/12/08/mallox-ransomware-showing-signs-of-increased-activity/

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**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

December 15, 2022 • 4:44 AM

More at www.hivepro.com