Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

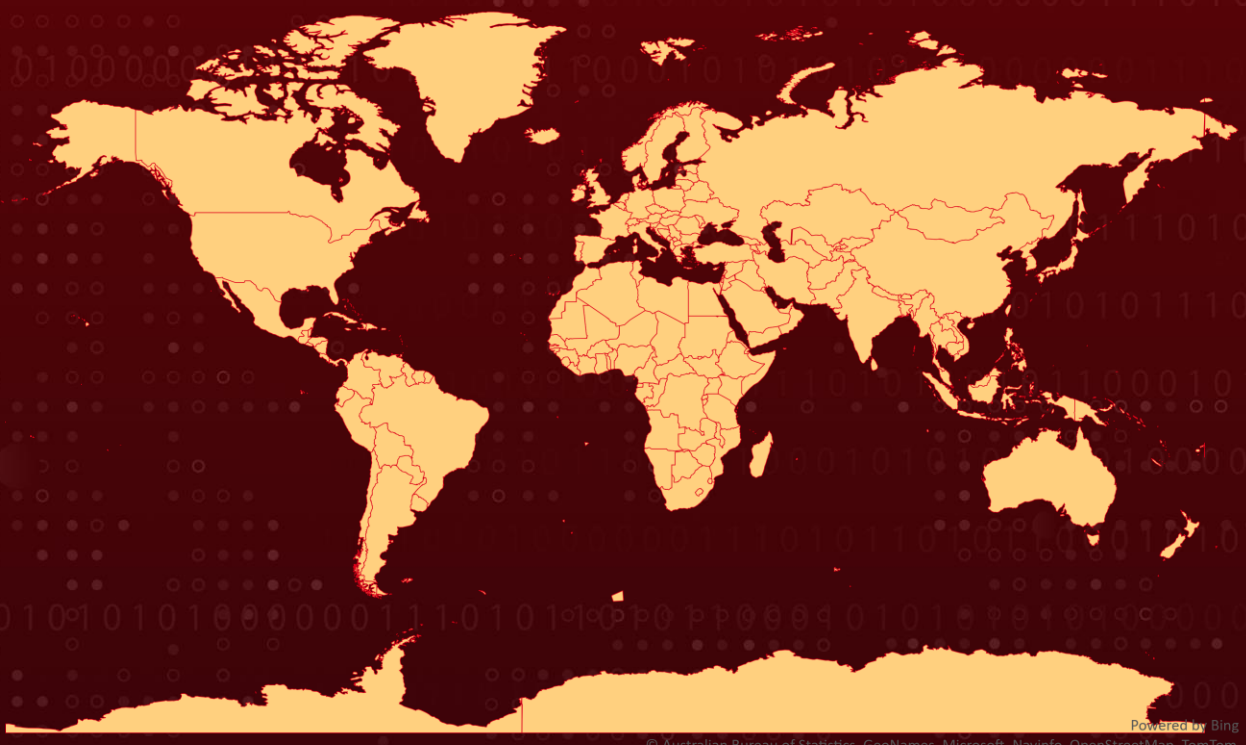
New Ransomware Variants Created Using Leaked Conti Source Code

Date of Publication	Admiralty Code	TA Number
December 28, 2022	A1	TA2022321

Summary

First appeared: February, 2020
Attack Region: Worldwide
Attack: The source code for the Conti ransomware has been leaked, and this has enabled the creation of new strains of ransomware.

Attack Regions



Attack Details

#1

The leaked source code of the Conti ransomware has been used to create new strains of the ransomware. These new strains include Putin Team, ScareCrow, BlueSky, and Meow ransomware are being distributed through various means, including email phishing campaigns and exploit kits. The new strains of ransomware are particularly virulent and have been used in attacks against a variety of organizations.

#2

The use of leaked source code to create new strains of ransomware is a relatively new development, and it may make it easier for hackers to create and distribute new strains of ransomware. Ransomware attacks can be disruptive and costly for organizations, as they can result in the loss of access to important data and systems, and may require the payment of a ransom to restore access.

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	**TA0040** Impact
T1204 User Execution	**T1129** Shared Modules	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1486** Data Encrypted for Impact	**T1204.001** Malicious Link	**T1105** Ingress Tool Transfer
T1588.001 Malware	**T1213** Data from Information Repositories		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	fe311979cd099677b1fd7c5b2008aed000f0e38d58eb3bfd30d04444476416f9 7f624cfb74685effcb325206b428db2be8ac6cce7b72b3edebbe8e310a645099 5a936250411bf5709a888db54680c131e9c0f40ff4ff04db4aeda5443481922f 7f6421cdf6355edfdcbddadd26bcdfbf984def301df3c6c03d71af8e30bb781f 222e2b91f5becea8c7c05883e4a58796a1f68628fbb0852b533fed08d8e9b853 b5b105751a2bf965a6b78eeff100fe4c75282ad6f37f98b9adcd15d8c64283ec
SHA1	94a9da09da3151f306ab8a5b00f60a38b077d594 987ad5aa6aee86f474fb9313334e6c9718d68daf 4f5d4e9d1e3b6a46f450ad1fb90340dfd718608b 578b1b0f46491b9d39d21f2103cb437bc2d71cac 5949c404aee552fc8ce29e3bf77bd08e54d37c59 59e756e0da6a82a0f9046a3538d507c75eb95252

TYPE	VALUE
MD5	4dd2b61e0ccf633e008359ad989de2ed 1d70020ddf6f29638b22887947dd5b9c 8f154ca4a8ee50dc448181afbc95cfd7 3eff7826b6eea73b0206f11d08073a68 033acf3b0f699a39becdc71d3e2dddcc 0bbb9b0d573a9c6027ca7e0b1f5478bf

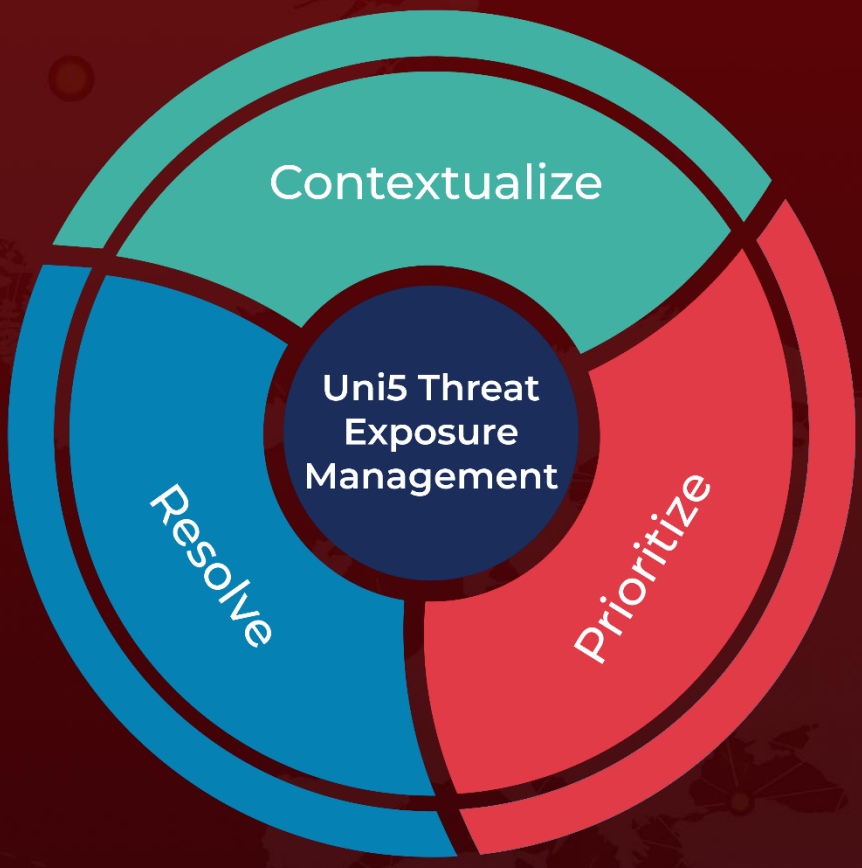
References

https://blog.cyble.com/2022/12/22/new-ransomware-strains-emerging-from-leaked-contis-source-code/

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

December 28, 2022 . 5:30 AM

More at www.hivepro.com