Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

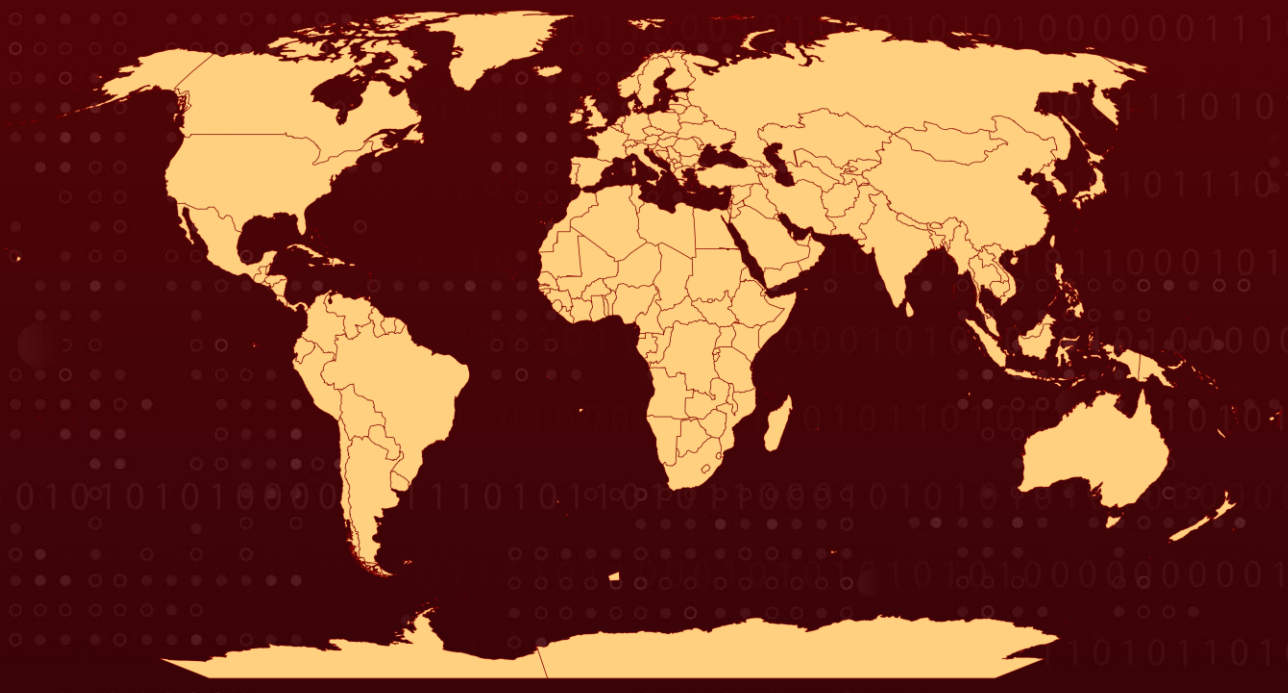
New Post-Exploitation Exfiltrator-22 Ransomware Framework Designed to Evade Detection

Date of Publication	Admiralty Code	TA Number
February 27, 2023	A1	TA2023105

Summary

First Appearance: November 2022
Target Countries: Worldwide
Attack: Exfiltrator-22 is a new post-exploitation framework for spreading ransomware and data theft. It is believed to be created by former LockBit 3.0 affiliates and is offered for a subscription fee ranging from $1,000 per month to $5,000 for lifetime access.

Attack Regions



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

Attack Details

#1 A new post-exploitation framework called EXFILTRATOR-22 a.k.a. EX-22 appears to have been created by a group operating in North, East, or South-East Asia. The group is skilled in defense evasion and anti-analysis techniques and is utilizing leaked source code to develop its own framework, which is being marketed as fully undetectable by every antivirus and endpoint detection and response vendor.

#2 The framework is being sold as a subscription-based service, with lifetime access costing $5,000 and per month $1000. The threat actors behind the framework have utilized domain fronting to conceal its command-and-control traffic, and similarities have been identified with a LockBit3.0 sample that has been actively used in LockBit3.0 campaigns.

#3 EXFILTRATOR-22 comes with a range of capabilities that allow an attacker to spread ransomware within corporate networks without being detected. Despite its high price, Exfiltrator-22 is expected to generate much interest in the cybercrime community, resulting in further code development and feature improvements.

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

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1129 Shared Modules	T1547 Boot or Logon AutoStart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information
T1055 Process Injection	T1134 Access Token Manipulation	T1497 Virtualization/Sandbox Evasion	T1055.003 Thread Execution Hijacking
T1112 Modify Registry	T1564 Hide Artifacts	T1564.003 Hidden Window	T1620 Reflective Code Loading
T1056 Input Capture	T1056.001 Keylogging	T1082 System Information Discovery	T1057 Process Discovery
T1083 File and Directory Discovery	T1497.002 User Activity-Based Checks	T1113 Screen Capture	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	32746688a23543e674ce6dcf03256d99988a269311bf3a8f0f944016fe3a931d d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee
SHA1	Eca49c8962c55bfb11d4dc612b275daa85cfe8c3 c2a321b6078acfab582a195c3eaf3fe05e095ce0

TYPE	VALUE
IPV4	23.216.147[.]76 20.99.184[.]37
MD5	874726830ae6329d3460767970a2f805 628e4a77536859ffc2853005924db2ef

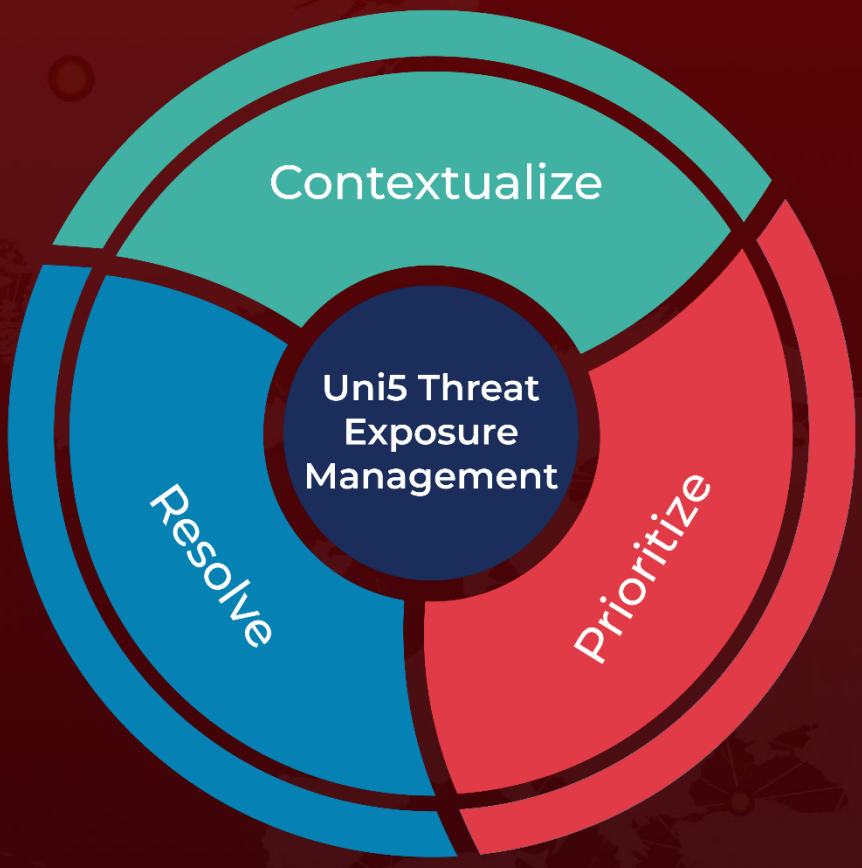
References

https://www.cyfirma.com/outofband/exfiltrator-22-an-emerging-post-exploitation-framework/

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 . 11:00 PM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com