Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

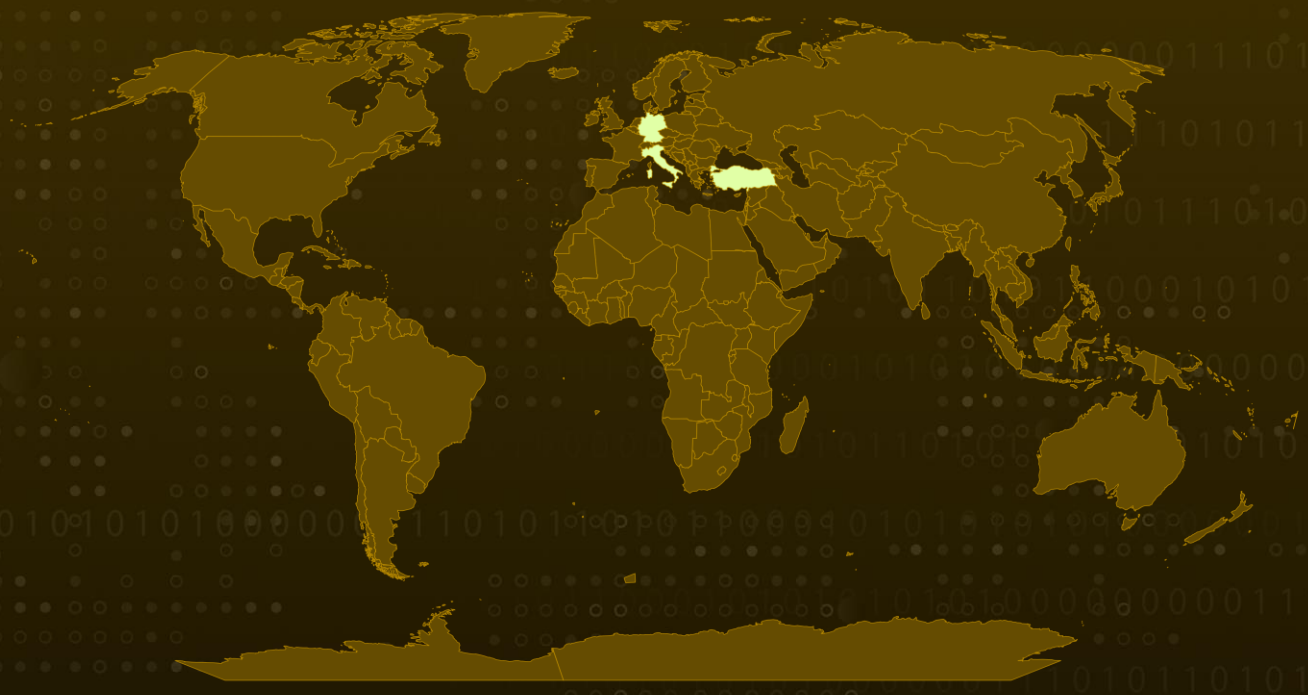
Campaigns Spread InfoStealer Malware Targeting Italy, Germany, and Turkey

Date of Publication	Admiralty Code	TA Number
December 26, 2022	A1	TA2022316

Summary

First appeared: December 6, 2022
Attack Region: Italy, Germany and Turkey
Attack Industry: Transportation
Attack: Multiple Campaigns Launched to Deploy Unknown InfoStealer Malware

Attack Regions



Attack Details

#1 A number of campaigns have been launched that spread InfoStealer malware written in the .NET programming language using phishing emails and Windows Shortcut (LNK) files and Batch Scripts (BAT). Based on the TTPs and evidence extracted, it appears the attacks were conducted by the same adversary (internally called AUI001).

#2 Though most of the attacks appear to have affected Italy, network visibility suggests similar implants also affected Germany and Turkey. This event/actor is also known as Alibaba2044 by some vendors based on a GitHub account used as a drop-point.

#3 There are several levels of obfuscation used in the final payload, hindering analysis and making it difficult to identify the specific family of malware. In some cases, it has been identified as PureLogs, a commercial infostealer. However, this final payload was also identified as zgRAT, a .NET RAT / InfoStealer.

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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0010 Exfiltration	T1566 Phishing	T1566.002 Spearphishing Link
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1204 User Execution
T1204.001 Malicious Link	T1204.002 Malicious File	T1140 Deobfuscate/Decode Files or Information	T1564 Hide Artifacts
T1564.001 Hidden Files and Directories	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1070 Indicator Removal
T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1055 Process Injection	T1055.002 Portable Executable Injection
T1082 System Information Discovery	T1083 File and Directory Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery
T1105 Ingress Tool Transfer	T1033 System Owner/User Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://raw[.]githubusercontent[.]com/alibaba2044/haul2/main/wininfo64.zip, hxxps://dl[.]dropboxusercontent[.]com/s/52eq2p19vc0dcei/IT_Fattura_n99392.zip, hxxps://downloadpdf-fattura[.]de/dpd/DOC9848-14-12-2022.zip

TYPE	VALUE
SHA256	2681a33478967ac0953785eac5f3b924c5159b6137ae96a619943c8dd1c8131b, 048159f1f7f087ed7704a7035cdcb8555ccb864e468a452e69c2d02864eb2ea1, 703fc33e07203b936f2cb2e24ee2ba40c1f07a998210617d16d511fcc0e207db, 32312ed6fc1968c041c331c74760d465897b28ccd939749949d07c23df063823, ccfa2a59f817a699433738eb52fef5e6aa236051fa68d6709e7b8a2c576c3de1, 8d4ed7017342c8b737b13f98b95956a5f3d2b2fcfbb921661d93a2c48a916911, d3aa8fca03e9eb9911bbb51302d703afa9c04ce94d94ce6c3cd5086999e49471, 752a84ba60cc53ec23642402ff87c1eee074ca6ae7703bec7b1ef9e600f63e9a, 32312ed6fc1968c041c331c74760d465897b28ccd939749949d07c23df063823, cbe92ec74d77f6524ddd4836b378b6e721db8f04f6d5f9df2a131d145d4f5bb8, a843517b019e86af42252b568e06dfe91a22f9034ceb996f5b0df32dcc1e4274, 6386dd85be2a3bd3529e8524c26cad7c4e8682f7dfcc25792a8db8f5d5d9528a, 048159f1f7f087ed7704a7035cdcb8555ccb864e468a452e69c2d02864eb2ea1
IPV4	116[.]203[.]19[.]97, 195[.]201[.]23[.]210
Domains	downloadpdf-fattura[.]de, utente[.]service-fatturecloud[.]de, service-fatturecloud[.]de

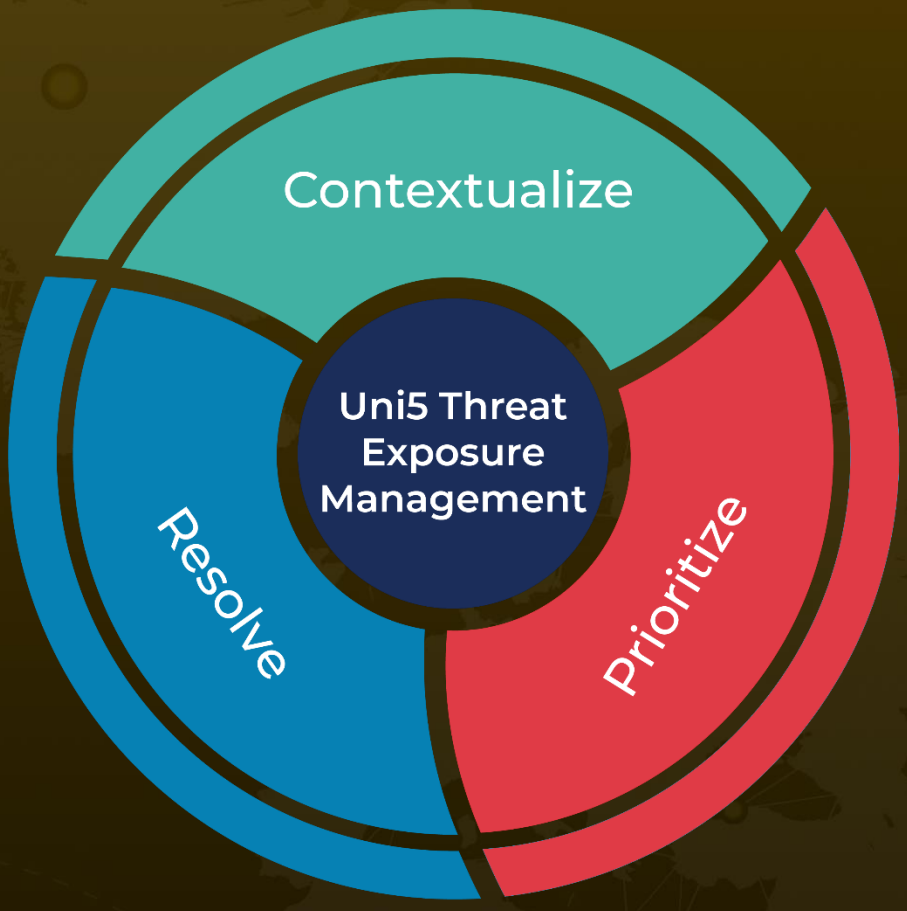
References

https://blog.cluster25.duskrise.com/2022/12/22/an-infostealer-comes-to-town

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 26, 2022 • 4:30 AM

More at www.hivepro.com