Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

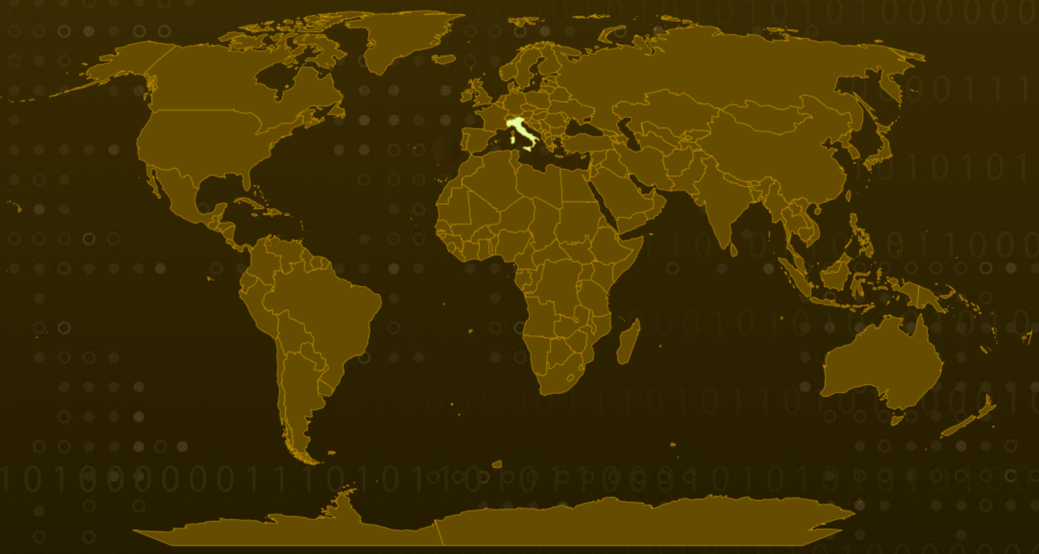
Gozi Malware Spreads through Fake Italian Revenue Agency Email Campaign

Date of Publication	Admiralty Code	TA Number
March 21, 2023	A1	TA2023148

Summary

Attack Began: March 2023
Attack Region: Italy
Malware: Gozi
Attack: A fake Italian Revenue Agency email campaign tricks victims into downloading a malicious attachment that installs Gozi, a binary that bypasses Italy's geofencing and creates a loader process on the victim's computer.

Attack Regions



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

Attack Details

#1

A recent malspam email campaign has been discovered impersonating the Italian Revenue Agency, luring victims into downloading and executing a malicious attachment. The attachment contains obfuscated code that, once unescaped and decoded, downloads an external payload that leverages the Curl command to bypass Italy's geofencing measures.

#2

The payload downloads a packed binary that contains a wrapper function for a decryption routine that calls the next shellcode, which then resolves API dynamically, creates a new memory section, and writes a loader process to disk. The binary has been identified as Gozi.

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	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information	T1056 Input Capture	T1005 Data from Local System
T1573 Encrypted Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	a3cec099b936e9f486de3b1492a81e55b17d5c2b06223f4256d49afc7bd212bc c99f4de75e3c6fe98d6fbbcd0a7dbf45e8c7539ec8dc77ce86cea2cfaf822b6a 9d1e71b94eab825c928377e93377feb62e02a85b7d750b883919207119a56e0d ebea18a2f0840080d033fb9eb3c54a91eb73f0138893e6c29eb7882bf74c1c30 df4f432719d32be6cc61598e9ca9a982dc0b6f093f8314c8557457729df3b37f 061c271c0617e56aeb196c834fcab2d24755afa50cd95cc6a299d76be496a858 876860a923754e2d2f6b1514d98f4914271e8cf60d3f95cf1f983e91baffa32b
IPV4	62[.]173[.]141[.]252 31[.]41[.]44[.]33 109[.]248[.]11[.]112

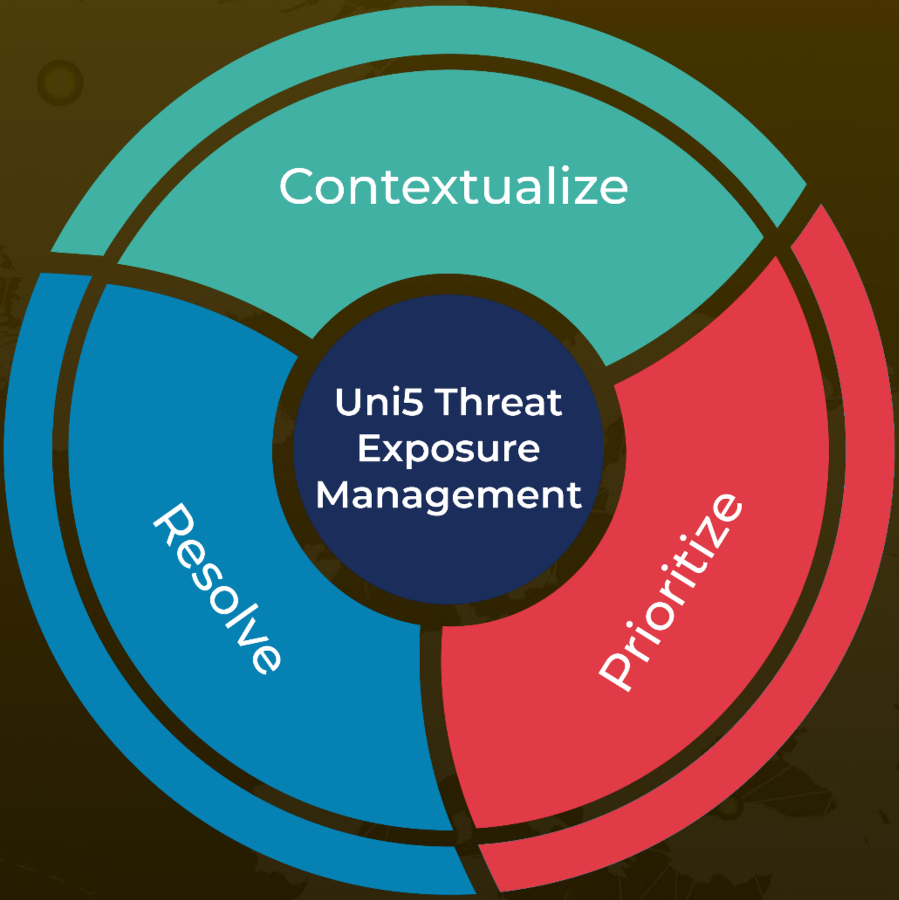
References

https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/gozi-italian-shellcode-dance

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

March 21, 2023 • 3:20 AM

More at www.hivepro.com