Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

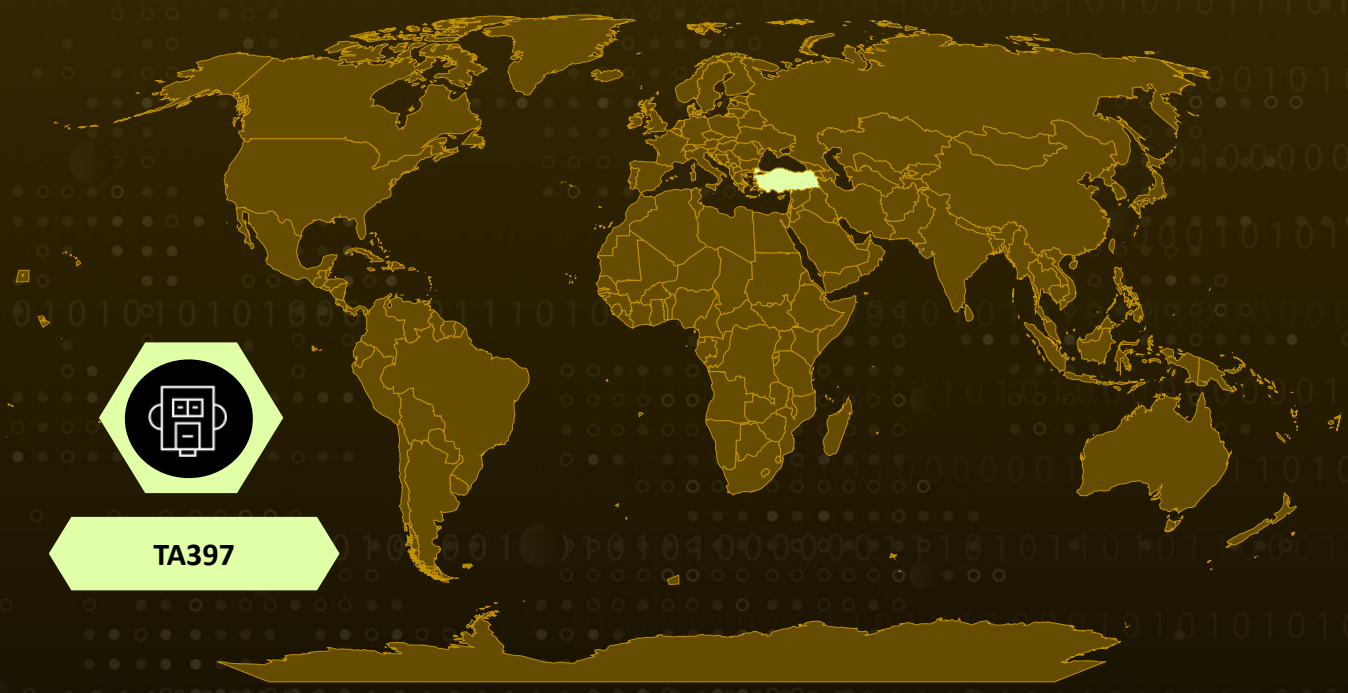
Uncovering TA397's Targeted Malware Campaign Against Turkish Defense

Date of Publication	Admiralty Code	TA Number
December 20, 2024	A1	TA2024468

Summary

First Seen: November 18, 2024
Targeted Country: Turkey
Malware: WmRAT and MiyaRAT
Threat Actor: TA397 (aka Bitter APT, T-APT-17, APT-C-08, Orange Yali)
Affected Platform: Windows
Targeted Industry: Defense
Attack: Threat actor TA397 targets organizations, especially in the Turkish defense sector, using spear-phishing emails with malicious LNK files disguised as infrastructure project documents. The attack chain installs WmRAT and MiyaRAT for espionage, leveraging scheduled tasks for stealthy payload delivery. This campaign underscores the need for robust email security and monitoring systems.

Attack Regions



Attack Details

#1 The recent campaign by threat actor TA397 employs a sophisticated attack chain targeting organizations, particularly within the Turkish defense sector. The attackers use spear-phishing emails containing a RAR archive that includes a malicious LNK file disguised as a legitimate document related to public infrastructure projects. Once the LNK file is executed, it sets up a scheduled task to download additional payloads.

#2 The payloads consist of espionage-focused remote access trojans (RATs), specifically WmRAT and MiyaRAT. These RATs enable attackers to remotely access and control compromised systems, facilitating intelligence gathering. This operation's techniques suggest a strategic focus on espionage to benefit government interests in South Asia.

#3 The use of LNK files and scheduled tasks allows the malware to operate stealthily, avoiding detection by traditional security solutions. The lure's relevance to infrastructure projects increases the likelihood of successful compromise within targeted organizations.

#4 TA397's approach reflects evolving strategies to exploit trusted processes for delivering malicious payloads. This campaign highlights the importance of enhanced email security, user awareness, and vigilant monitoring for unusual task scheduling activity.

Recommendations

- **Endpoint Protection:** Deploy advanced endpoint detection and response (EDR) tools to identify suspicious activities like unusual scheduled tasks or LNK file executions.
- **Email Security:** Implement robust email security filters to detect and block spear-phishing attempts, particularly those using infrastructure-related lures.
- **Access Control:** Restrict execution permissions for script-based files and LNK files where possible.
- **Network Monitoring:** Monitor for unusual network traffic or connections associated with RAT activity and block known malicious IP addresses or domains.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0003 Persistence	TA0009 Collection	TA0011 Command and Control
T1053 Scheduled Task/Job	T1047 Windows Management Instrumentation	T1041 Exfiltration Over C2 Channel	T1027 Obfuscated Files or Information
T1204.001 Malicious Link	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1053.005 Scheduled Task
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204 User Execution	T1564 Hide Artifacts
T1614 System Location Discovery	T1113 Screen Capture	T1204.002 Malicious File	T1217 Browser Information Discovery
T1056.001 Keylogging	T1056 Input Capture		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	53a653aae9678075276bdb8ccf5eaff947f9121f73b8dcf24858c0447922d0b1, f6c77098906f5634789d7fd7ff294bfd95325d69f1be96be1ee49ff161e07733, 10cec5a84943f9b0c635640fad93fd2a2469cc46aae5e43a4604c903d139970f, C7ab300df27ad41f8d9e52e2d732f95479f4212a3c3d62dbf0511b37b3e81317

TYPE	VALUE
Domains	academymusica[.]com, samsnewlooker[.]com, jacknwoods[.]com
IPv4	38[.]180[.]142[.]228, 96[.]9[.]215[.]155

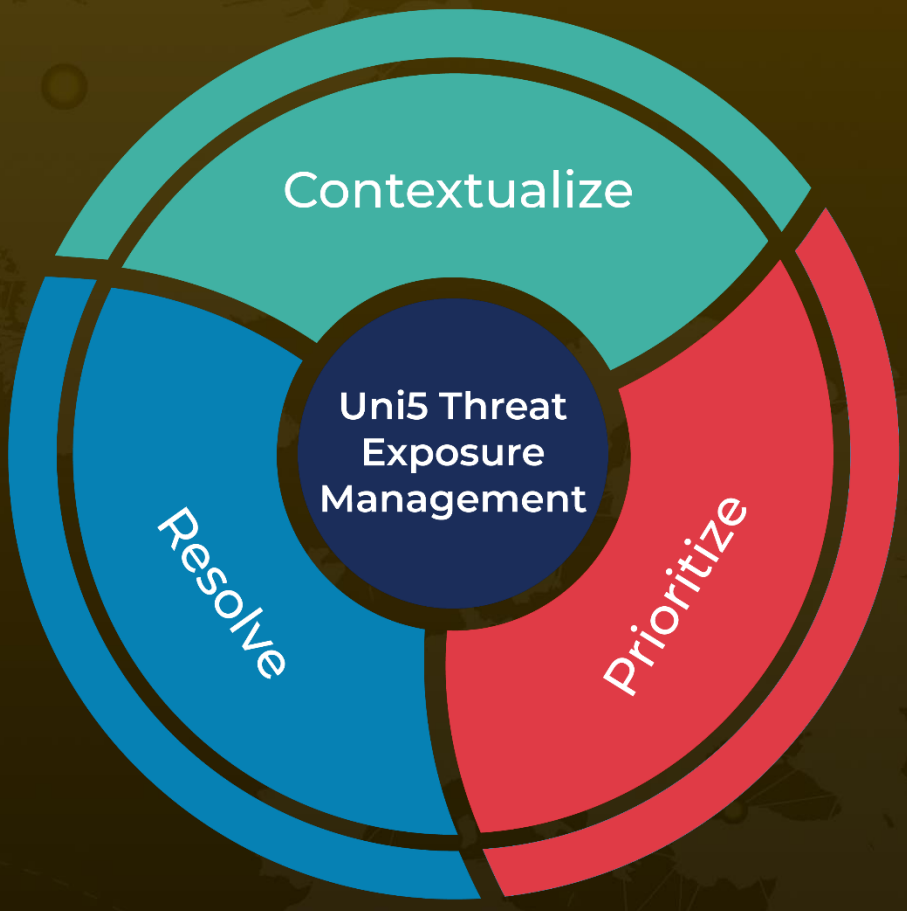
References

https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats

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 20, 2024 • 3:30 AM

More at www.hivepro.com