Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

APT17's Espionage Surge: Italian Targets Hit by 9002 RAT

Date of Publication	Admiralty Code	TA Number
July 18, 2024	A1	TA2024277

Summary

Attack Commenced: June 2024
Threat Actor: APT17 (aka Tailgater Team, Elderwood, Elderwood Gang, Sneaky Panda, SIG22, Beijing Group, Bronze Keystone, TG-8153, TEMP.Avengers, Dogfish, Deputy Dog, ATK 2)
Malware: 9002 RAT (aka McRAT, Hydraq, HOMEUNIX)
Attack Region: Italy
Targeted Industries: Business, Government
Attack: In June and July 2024, APT17 escalated its cyber espionage activities, targeting Italian companies and government entities with the 9002 RAT malware. This China-linked threat actor used sophisticated phishing campaigns to achieve their objectives.

Attack Regions

Attack Details

#1 The attacks on June 24 and July 2, 2024, signify a worrisome escalation in cyber espionage activities by APT17, also known as DeputyDog. This China-linked threat actor targeted Italian companies and government entities using a variant of the notorious 9002 RAT malware.

#2 The first campaign utilized an Office document, while the second campaign employed a malicious link. In both cases, the attackers cleverly disguised their phishing attempts as invitations to install a Skype for Business package from a seemingly legitimate Italian government domain, thereby deploying the 9002 RAT.

#3 The 9002 RAT, a Remote Access Tool, is typically used by APTs to gain control over a victim's machine. The infection chain begins with a phishing email containing a link or DOCX file that directs the victim to a malicious website. Here, a harmful installer file is downloaded and executed, running a Visual Basic script (vcruntime.vbs), which subsequently executes a Java application.

#4 This Java application creates and runs a shellcode to install the 9002 RAT on the victim's system, granting the attackers remote control. The 9002 RAT communicates with a Command and Control (C&C) server to receive instructions and exfiltrate data.

#5 Beyond facilitating network traffic monitoring and screenshot capturing, the 9002 RAT also enables process management, file enumeration, and command execution. One of its most sinister features is its ability to regularly update itself, including utilizing diskless variations that operate entirely in memory, making it much harder to detect.

Recommendations

Email Security: Implement advanced email filtering and phishing detection systems to block malicious attachments and URLs. Educate employees about phishing tactics and encourage cautious handling of email attachments and links.

Monitor and Analyze Security Logs: Implement centralized logging to gather security logs from across your network and endpoints and use Security Information and Event Management (SIEM) solutions to correlate and analyze this data for signs of suspicious activity.

Enhance Network Security: Segment your network to limit lateral movement and reduce breach impact, while employing network monitoring tools to detect unusual traffic patterns and communication with known Command and Control (C&C) servers.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Verify Software Integrity: Regularly check the hashes of downloaded installer files against official sources or vendor-provided checksums to ensure they have not been tampered with or replaced with malicious versions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1113** Screen Capture
T1041 Exfiltration Over C2 Channel	**T1083** File and Directory Discovery	**T1007** System Service Discovery	**T1005** Data from Local System
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1566.002** Spearphishing Link	**T1059** Command and Scripting Interpreter
T1059.005 Visual Basic	**T1204** User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File
T1656 Impersonation	**T1036** Masquerading	**T1562** Impair Defenses	**T1056** Input Capture

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	themicrosoftnow[.]com, meeting[.]equitaligaiustizia[.]it
IPv4	137[.]74[.]76[.]92, 23[.]218[.]225[.]10
SHA256	28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e, e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c, d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436, c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c, caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5, de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0

References

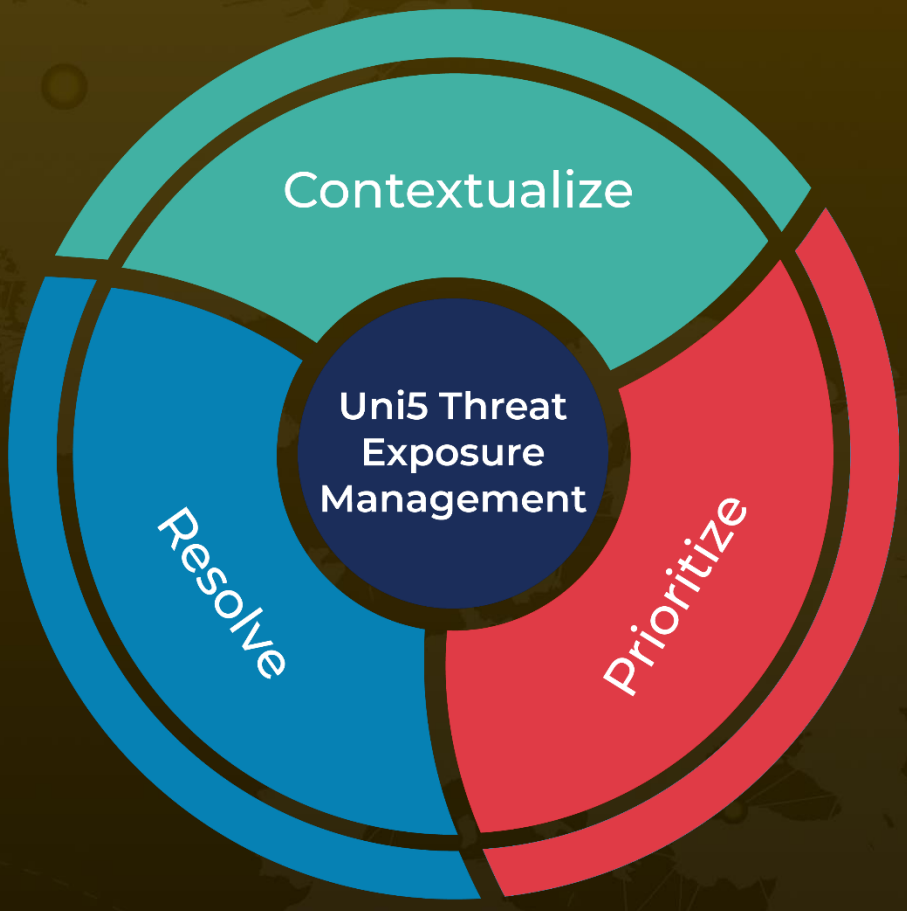
https://www.tgsoft.it/news/news_archivio.asp?id=1557&lang=eng

https://attack.mitre.org/groups/G0025/

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

July 18, 2024 • 10:00 PM

More at www.hivepro.com