Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

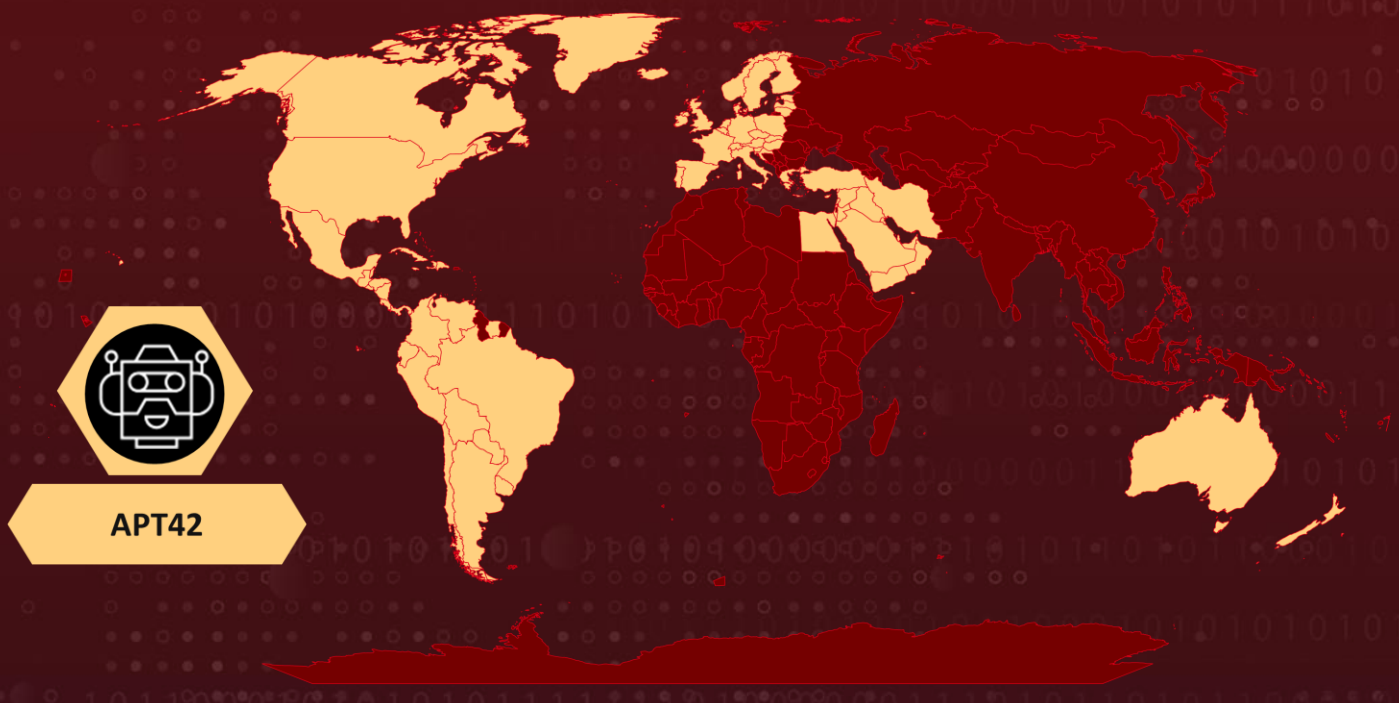
APT42’s Operations Employ "Nicecurl" and "Tamecat" Malwares

Date of Publication	Admiralty Code	TA Number
May 6, 2024	A1	TA2024173

Summary

Attack Began: May 2024
Attack Region: Western and Middle Eastern
Affected Industries: NGOs, media organizations, academia, legal services, researchers, journalists, defense, foreign affairs
Actor: APT42 (aka UNC2448)
Malware: Nicecurl, Tamecat
Attack: APT42 has been observed targeting entities in both the Middle East and Western regions, infiltrating their cloud environments and corporate networks using social engineering techniques, particularly by impersonating journalists. Using malicious emails as their primary vector, APT42 infects recipients with two distinct backdoors known as "Nicecurl" and "Tamecat." Once deployed within the compromised systems, these backdoors provide the attackers with capabilities for data exfiltration and command execution.

Attack Regions



Attack Details

#1 APT42 is a cyber espionage group hailing from Iran and linked to the Islamic Revolutionary Guard Corps (IRGC). They're notorious for their targeted cyber attacks on various sectors, including NGOs, media outlets, academia, legal services, and activists. They often pretend to be journalists or event organizers to gain access to victim networks, including cloud systems. By building trust through correspondence and invitations to fake conferences, they manage to harvest credentials and infiltrate cloud environments.

#2 Their primary goal is to quietly extract strategic data valuable to Iran. They achieve this by using built-in features and open-source tools to avoid detection. Recently, they've been deploying custom backdoors like NICECURL and TAMECAT through spear phishing campaigns.

#3 APT42 operates through three infrastructure clusters to gather credentials. Each cluster employs similar tactics but with varied domains and themes to stay under the radar. In Cluster A, APT42 focuses on journalists, researchers, and geopolitical entities within Iran's sphere of interest. They pretend to be news outlets or NGOs, sending spear phishing emails with malicious links leading to fake Google login pages.

#4 Cluster B sees APT42 using domains like .top, .online, .site, and .live to pose as legitimate services. Their spear phishing emails often contain invitations to conferences or documents hosted on cloud platforms. APT42's clever use of typo-squatted domains to redirect victims to fake login pages. They've targeted freelance journalists and activists, among others.

#5 Cluster C, active since 2022, targets defense, foreign affairs, and academic sectors in the U.S. and Israel. They use disguises like "Mailer Daemon" and URL shortening services to distribute phishing links.

#6 In January 2024, a malicious file was discovered downloading the backdoors alongside a decoy PDF. NICECURL is a VBScript-based backdoor capable of downloading supplementary modules for execution, such as data mining and arbitrary command execution. TAMECAT, on the other hand, is a PowerShell-based foothold that enables the execution of arbitrary PowerShell or C# content. APT42 remains focused on intelligence collection, deploying customized implants and engaging in extensive cloud operations.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
T1598 Phishing for Information	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1059.007 JavaScript
T1059.005 Visual Basic	T1059.001 PowerShell	T1566 Phishing	T1566.002 Spearphishing Link
T1027 Obfuscated Files or Information	T1573 Encrypted Channel	T1105 Ingress Tool Transfer	T1047 Windows Management Instrumentation
T1204 User Execution	T1204.001 Malicious Link	T1036 Masquerading	T1056 Input Capture

T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1537** Transfer Data to Cloud Account	**T1140** Deobfuscate/Decode Files or Information
T1555 Credentials from Password Stores			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	azadlliq[.]info, businessInsider[.]org, ecomonist[.]org, eocnomist[.]com, foreiqnaffairs[.]com, forieqnaffairs[.]com, foreiqnaffairs[.]org, israelhayum[.]com, jpost[.]press, jpostpress[.]com, khaleejtimes[.]org, khalejtimes[.]org, maariv[.]net, themedealine[.]org, timesfisrael[.]com vanityfaire[.]org washinqtonpost[.]press, ynetnews[.]press, account-signin[.]com, acconut-signin[.]com, accounts-mails[.]com, coordinate[.]icu, dloffice[.]top, dloffice[.]buzz, myaccount-signin[.]com, signin-acconut[.]com, signin-accounts[.]com, signin-mail[.]com, signin-mails[.]com, signin-myaccounts[.]com, support-account[.]xyz, accredit-validity[.]online, activity-permission[.]online, admin-stable-right[.]top, admiscion[.]online,

TYPE	VALUE
Domain	book-download[.]shop, bq-ledmagic[.]online, briview[.]online, chat-services[.]online, check-online-panel[.]live, check-pabnel-status[.]live, check-panel-status[.]live, check-panel-status[.]live, check-short-panel[.]live, confirmation-process[.]top, connection-view[.]online, continue-meeting[.]site, continue-recognized[.]online, cvisiion[.]online, drive-access[.]site, endorsement-services[.]online, fortune-retire-home[.]top, geaviews[.]site, glory-uplift-vouch[.]online, go-conversation[.]lol, go-forward[.]quest, gview[.]site, home-continue[.]online, home-proceed[.]online, identifier-direction[.]site, indication-service[.]online, join-paneling[.]online, ksview[.]top, last-check-leave[.]buzz, live-project-online[.]live, live-projects-online[.]top, loriginal[.]online, mail-roundcube[.]site, meeting-online[.]site, mterview[.]site, nterview[.]site, online-processing[.]online, online-video-services[.]site, affect-fist-ton[.]online, avid-striking-eagerness[.]online, beaviews[.]online, besvision[.]top, bloom-flatter-affably[.]top, admit-roar-frame[.]top, advission[.]online,

TYPE	VALUE
Domain	panel-views-cheking[.]live, panelchecking[.]live, paneling-viewing[.]live, panels-views-ckeck[.]live, pannel-get-data[.]us, quomodocunquize[.]site, recognize-validation[.]online, reconsider[.]site, revive-project-live[.]online, short-url[.]live, short-view[.]online, shortenurl[.]online, shortingurling[.]live, shortlinkview[.]live, shortulonline[.]live, shorting-ce[.]live, shoting-urls[.]live, simple-process-static[.]top, status-short[.]live, stellar-roar-right[.]buzz, sweet-pinnacle-readily[.]online, tcvision[.]online, title-flow-store[.]online, twision[.]top, ushrt[.]us, verify-person-entry[.]top, view-cope-flow[.]online, view-panel[.]live, view-pool-cope[.]online, view-total-step[.]online, viewstand[.]online, viewtop[.]online, virtue-regular-ready[.]online, we-transfer[.]shop, m85[.]online, s51[.]online, s59[.]site, s20[.]site, d75[.]site, bitly[.]org[.]il, litby[.]us, daemon-mailer[.]co, daemon-mailer[.]info, email-daemon[.]biz, email-daemon[.]biz[.]tinurls[.]com, email-daemon[.]online[.]tinurls[.]com, email-daemon[.]online,

TYPE	VALUE
Domain	email-daemon[.]site, mailer-daemon[.]info, mailerdaemon[.]online, mailer-daemon[.]us, aspenInstitute[.]org, mccainInstitute[.]org, washingtonInstitute[.]org, youtransfer[.]live, g-online[.]org, online-access[.]live, ovcloud[.]online, panel-check-short[.]live, panel-check-short[.]live, panel-live-check[.]online, panel-short-check[.]live, panel-view-short[.]online, panel-view[.]live, panel-view[.]online, youronlineregister[.]com
MD5	d5a05212f5931d50bb024567a2873642, 347b273df245f5e1fcbef32f5b836f1d, 2f6bf8586ed0a87ef3d156124de32757, 13aa118181ac6a202f0a64c0c7a61ce7, c23663ebdfbc340457201dbec7469386, 853687659483d215309941dae391a68f, d7bf138d1aa2b70d6204a2f3c3bc72a7, 081419a484bbf99f278ce636d445b9d8, c3b9191f3a3c139ae886c0840709865e, dd2653a2543fa44eaeeff3ca82fe3513, 9c5337e0b1aef2657948fd5e82bdb4c3
URL	drive-file-share[.]site, prism-west-candy[.]glitch[.]me, tnt200[.]mywire[.]org, accurate-sprout-porpoise[.]glitch[.]me

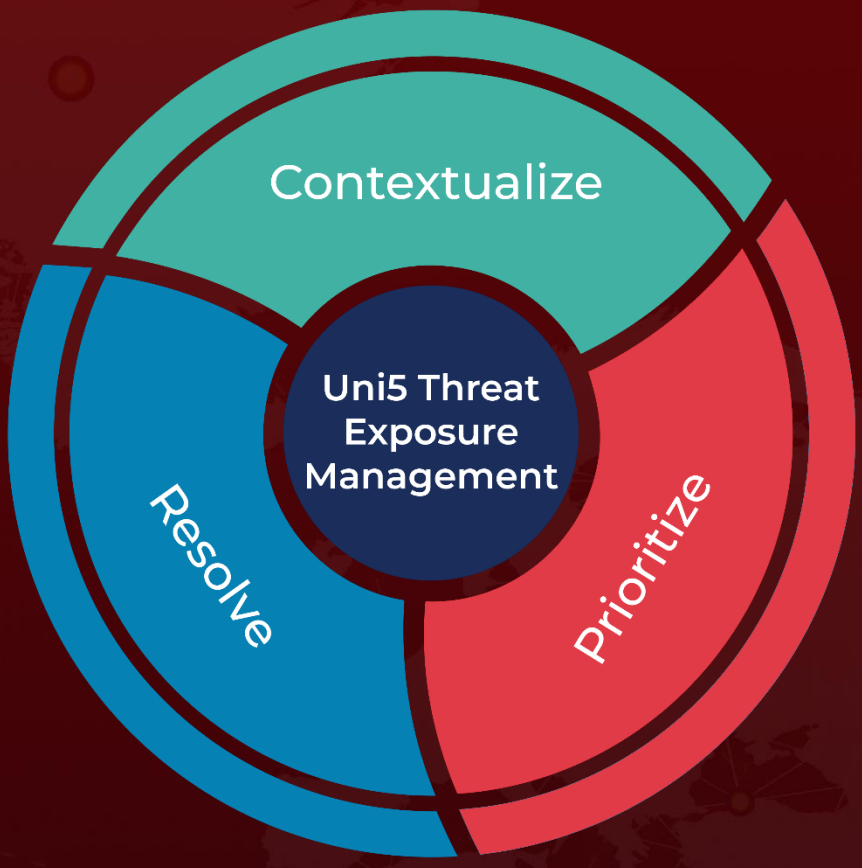
References

https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

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

May 6, 2024 • 6:30 AM

More at www.hivepro.com