APT42's recent activity

Original report published on: May 02, 2024[1]

Executive Summary

Google Cloud unveiled tactics belonging to an Iranian state-sponsored cyber espionage group, APT42, which employed social engineering techniques to target Western and Middle Eastern media companies, non-governmental organisations, academia, legal services and activist groups.

Recent malware operations by APT42 involve custom backdoors such as NICECURL and TAMECAT, typically delivered via spear phishing. These backdoors grant initial access and act as interfaces for command execution or launch points for further malware development.

Background

Since 2021, APT42 has impersonated well-known news outlets and employed typo squatting to create web domains that closely resemble legitimate ones with minor alterations. The group has remained relatively focused on intelligence gathering, using these techniques to obtain credentials and strategic information. They built trust by impersonating journalists and event organisers, sending realistic conference invitations or documents to gather credentials and access cloud environments. They then discreetly exfiltrate important data, using built-in features and open-source tools to evade detection.

It is well documented that APT42 uses the following custom backdoors:

- ***NICECURL*** is a backdoor written in VBScript that can download additional modules to be executed, including data mining and arbitrary command execution. The backdoor's accepted commands include "kill" to remove artifacts and end execution, "SetNewConfig" to set a new sleep value, and "Module" to download and execute additional files, potentially extending NICECURL's functionality. NICECURL communicates over HTTPS.

- ***TAMECAT*** is a PowerShell toehold that can execute arbitrary PowerShell or C# content. TAMECAT is dropped by malicious macro documents, communicates with its command-and-control (C2) node via HTTP, and expects data from the C2 to beBase64 encoded. Mandiant previously observed TAMECAT used in a large-scale APT42 spear-phishing campaign targeting individuals or entities employed by or affiliated with NGOs, government, or intergovernmental organisations around the world.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny/disable processes, ports and protocols that have no business need.
- Deploy a multi-layered protection solution that includes email sandboxing, domain URL filtering, endpoint detection and response protection, and network security measures to detect and block phishing attempts and other threats at various entry points.

- Deploy data loss prevention solution to monitor that data remains within the enterprise or approved networks.
- Be alert for suspicious emails, particularly those containing phishing attempts or malicious attachment and educate employees on social engineering tactics used by APTs.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise[1]

SHA256 Hash	Description
e0ba0cedd8a8624c75af29965e5fa7ab754fc0fcddbb330bb548dab4f2be333f	NICECURL
0e51029ba28243b0a6a071713c17357a8eb024aa4298d1ccc9e2c4ac8916df4d	
3226b3e7d7fdaebfe7d7f06bdaf0cad08ea9792cd32843d01e6023f67cd0c889	
3c74109005111688341f4e5fcba42be9c21baa4465f5f84a5a342708732ac0ff	
dbdb14e37fc4412711a1e5e37e609e33410de31de13911aee99ab473753baa4a	
07384ab4488ea795affc923851e00ebc2ead3f01b57be6bf8358d7659e9ee407	
5404e39f2f175a0fc993513ee52be3679a64c69c79e32caa656fbb7645965422	TAMECAT
bd1f0fb085c486e97d82b6e8acb3977497c59c3ac79f973f96c395e7f0ca97f8	
156ac9685acb6696d8d7f64205e20ecf7a87dad304b8441449f0060ed175938b	
c99cc10f15f655f36314e54f7013a0bc5df85f4d6ff7f35b14a446315835d334	

MD5 Hash	Description
9c5337e0b1aef2657948fd5e82bdb4c3	TAMECAT

Domain	Description
azadlliq[.]info	Posing as News Outlets
businesslnsider[.]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	Posing as Legitimate Services
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	Posing as Generic Login Services
admin-stable-right[.]top	
admiscion[.]online	
admit-roar-frame[.]top	
advission[.]online	
affect-fist-ton[.]online	
avid-striking-eagerness[.]online	
beaviews[.]online	
besvision[.]top	
bloom-flatter-affably[.]top	
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	
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	
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	URL Shortening Services
s51[.]online	
s59[.]site	
s20[.]site	
d75[.]site	
bitly[.]org[.]il	
litby[.]us	
daemon-mailer[.]co	Mailer Daemon
daemon-mailer[.]info	
email-daemon[.]biz	
email-daemon[.]biz[.]tinurls[.]com	
email-daemon[.]online[.]tinurls[.]com	
email-daemon[.]online	
email-daemon[.]site	

mailer-daemon[.]info	
mailerdaemon[.]online	
mailer-daemon[.]us	
aspenInstitute[.]org	Posing as Think Tanks & Research Institutes
mccainInstitute[.]org	
washingtonInstitute[.]org	
youtransfer[.]live	File Sharing Services
g-online[.]org	Miscellaneous
online-access[.]live	
youronlineregister[.]com	

MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1566.002	Phishing: Spearphishing Link
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.007	Command and Scripting Interpreter: JavaScript
Persistence	T1098.005	Account Manipulation: Device Registration
Defense Evasion	T1027	Obfuscated Files or Information
	T1070	Indicator Removal: File Deletion
Discovery	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel

References

1. ^ “UNCHARMED: UNTANGLING IRAN'S APT42 OPERATIONS”