COPY KITTENS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON COPY KITTENS: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.

II. TARGETS

This threat actor targets government institutions, universities, defense contractors, and large IT companies for the purpose of espionage.
The main countries targeted by CopyKittens are Israel, Saudi Arabia, Turkey, the U.S., Jordan and Germany. Within these countries, the targets vary - with government institutions, defense companies, sub-contractors and large IT companies among the most targeted organizations.

III. METHODS USED

CopyKittens use several self-developed malware and hacking tools that have not been publicly reported till 2017, and are analyzed in Clearsky report: TDTESS backdoor; Vminst, a lateral movement tool; NetSrv, a Cobalt Strike loader; and ZPP, a files compression console program. The group also uses Matryoshka v1, a self developed RAT analyzed by ClearSky in the 2015 report, and Matryoshka v2 which is a new version, albeit withsimilar functionality. The group often uses the trial version of Cobalt Strike3 , a publicly available commercial software for "Adversary Simulations and Red Team Operations." states the report

IV. CAMPAIGNS

- **2015** : In the middle of 2015, Dr. Gindin received numerous spear-phishing emails, one of which contained malware while three others contained links to fake login pages. This was only the beginning. Messages from unknown senders suddenly poured into her Facebook inbox. Hackers launched brute-force attacks, abusing recovery options to take over her cloud accounts. On two separate occasions, attackers even befriended her via phone hoping to get additional details they can use in more phishing emails.

- **2017 (operation wilted tulip)**: CopyKittens has conducted at least three waves of cyber-attacks in the past year. In each of the attacks the infection method was almost identical and included an extraordinary number of stages used to avoid detection. As with other common threat actors, the group relies on social engineering methods to deceive its targets prior to infection.
- **On 30 March 2017**, ClearSky reported a breach of multiple websites, such as Jerusalem Post, Maariv news and
- **On 26 April 2017**, a malicious email was sent from an employee account that was likely breached within the Ministry of Northern Cyprus. It was sent to a disclosed recipients list in government institutions in several countries and other organizations, mostly in or related to ministries of foreign affairs. We should note, however, that it is possible that the attackers were interested only in a few of the recipient organizations, but sent it to a wider list because they showed up in previous correspondences in the breached account.

AX1AL

V. IOCS

MD5/SHA 256 Hashes

- a60a32f21ac1a2ec33135a650aa8dc71
- 94ba33696cd6ffd6335948a752ec9c19
- bcae706c00e07936fc41ac47d671fc40
- 1ca03f92f71d5ecb5dbf71b14d48495c
- 506415ef517b4b1f7679b3664ad399e1
- 1ca03f92f71d5ecb5dbf71b14d48495c
- bd38cab32b3b8b64e5d5d3df36f7c55a
- ac29659dc10b2811372c83675ff57d23
- 41466bbb49dd35f9aa3002e546da65eb
- 8f6f7416cfdf8d500d6c3dcb33c4f4c9e1cd33998c957fea77fbd50471faec88
- 02f2c896287bc6a71275e8ebe311630557800081862a56a3c22c143f2f3142bd
- 2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9
- 55f513d0d8e1fd41b1417a0eb2afff3a039a9529571196dd7882d1251ab1f9bc
- da529e0b81625828d52cd70efba50794
- 1f9910cafe0e5f39887b2d5ab4df0d10
- 0feb0b50b99f0b303a5081ffb3c4446d
- 577577d6df1833629bfd0d612e3dbb05
- 165f8db9c6e2ca79260b159b4618a496e1ed6730d800798d51d38f07b3653952
- 1f867be812087722010f12028beeaf376043e5d7
- b571c8e0e3768a12794eaf0ce24e6697
- e319f3fb40957a5ff13695306dd9de25
- acf24620e544f79e55fd8ae6022e040257b60b33cf474c37f2877c39fbf2308a

C2's / Domains / IP'S

209.190.20.147
209.190.20.149
209.190.20.148
img.gmailtagmanager[.]com
windowkernel[.]com
windowslayer[.]in
windowkernel[.]com
wheatherserviceapi[.]info
wethearservice[.]com
windowslayer[.]in
u[.]mywindows24[.]in
main[.]windowskernel14[.]com
walla[.]link
heartax[.]info
haaretz[.]link
Haaretz-News[.]com
gmailtagmanager[.]com
fbstatic-a[.]xyz
fbstatic-a[.]space
fbstatic-akamaihd[.]com
alhadath[.]mobi
big-windowss[.]com
kernel4windows[.]in
micro-windows[.]in
mywindows24[.]in
patch7-windows[.]com
patch8-windows[.]com
patchthiswindows[.]com
windows-10patch[.]in
windows-drive20[.]com

TTP's

Victims are targeted via several methods, including spear phishing emails, watering hole attacks, fake social media profiles and targeting exposed webmail accounts.
The group uses a combination of these methods to persistently target the same victim over multiple platforms until they succeed in establishing an initial beachhead of infection - before pivoting to higher value targets on the network.To do this the group leverages their own custom malware tools in combination with existing, commercial tools, such as Cobalt Strike and Metasploit.

VI. References / Sources

https://attack.mitre.org/groups/G0052/
https://www.cfr.org/cyber-operations/copykittens
https://securityaffairs.co/wordpress/61363/apt/copykittens-operation-wilted-tulip.html
https://malpedia.caad.fkie.fraunhofer.de/actor/copykittens
https://blog.trendmicro.com/trendlabs-security-intelligence/the-spy-kittens-are-back-an-update-to-rocket-kitten/
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://blog.trendmicro.com/copykittens-exposed-clearsky-trend-micro/
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf