CONFUCIUS

AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Confucius is a threat actor from India and has been primarily active since 2013. Their prime motivation was Information Theft and Cyber-Espionage. Previously they were seen abusing Yahoo and Quora forums as a part of their C2 communications. Their operations include deploying backdoors and stealing files with a tailored file stealer. The group seems to be associated with Patchwork and Dropping Elephant.

II. TARGET SECTORS

Confucius targets include Mongolia, Pakistan, Trinidad and Tobago, Ukraine, SEA Region, Middle East Region and African Countries.

III. METHODS USED

Confucius developed multiple chat software for Windows and Android based on a legitimate, opensource chat application. The chat applications they developed have backdoor functionalities. They had also used Social Engineering. Their backdoors are delivered through Office documents exploiting memory corruption vulnerabilities CVE-2015-1641 and CVE-2017-11882

IV. OPERATIONS

- In 2017, Palo Alto's Unit42 had discovered three documents crafted to exploit the InPage program. The decoy documents used by the InPage exploits suggest that the targets are likely to be politically or militarily motivated. They contained subjects such as intelligence reports and political situations related to India, the Kashmir region, or terrorism being used as lure documents. The Documents drop Confucius_B malware family, Backdoor.BioData and Backdoor.MY24.
- Also in the Same Year, Trend Micro did an in-depth analysis on Confucius' Infrastructure and found out websites offering Windows and Android chat applications namely, Secret Point Chat, and Tweety Chat.
- In 2018, Palo Alto's Unit42 discovered that Confucius had set up two new websites and new payloads with which to compromise its targets. ‘CONFUCIUS_A’, a malware family that has links to a series of attacks associated with a backdoor attack method commonly known as SNEEPY (aka ByeByeShell) and ‘CONFUCIUS_B’, which has a loose link to the series of attacks associated with Operation Patchwork and The Hangover Report.
- In 2021, Uptycs Threat Research Team discovered an ongoing targeted attack campaign with Warzone RAT. The decoy lure was a 16-page document that would have skipped out of static heuristic engines sights because they generally scan suspicious files based on the number of pages. Upon execution, the document used template injection to download the next stage exploit that downloaded the final stage Warzone payload.

V. IOC

SHA256

- 8cfd559756630d967bb597b087af98adc75895a1ec52586d53a2d898e4a6e9b0
- fb9064abd562012f7c4ffec335f1b669d7ffa0ce724b81f83840474e544c0113
- ec15a7698eed7a925b0c074239a92b9f3efdd1054ea281fa914c0bf63d73d319
- 09fcb9444b415781d1d01d0b43c37df441a381042a3f2f91f04890b9c4632c5e
- 487d43f38006a609715f95d2e8dd605446de820cafcc453d57a452bc67972a7a
- 7b9454ac9c96db562c2b961a72aa1fece896cd1633a1ec3139eb75346a086f64
- d0176a1d30827a42dda4f575ede0d2d8ad0f71306e41f67b1d1fe999f0e82838
- dd34f8236b314ce5123fc036c7ae1d0b4ef6da3ae781d639bcc1d5a30b197b2c
- c975954fbb473ed8ce3a98ca2c4977bf22d2413db01eda87599524969565836f
- 1220815b09694b522a33a4feacfc20ca90e03728c9f5e2bd4288e67e2e1257de
- 1b682fa08d99b1f57e545cab2e0cd553282682f7706a72afe5ee63264002e010
- b9b5a9fa0ad7f802899e82e103a6c2c699c09390b1a79ae2b357cacc68f1ca8e
- 2f5fc653550b0b5d093427263b26892e3468e125686eb41206319c7060212c40
- 07277c9f33d0ae873c2be3742669594acc18c7aa93ecadb8b2ce9b870baceb2f
- 4500851dad1ac87165fc938fe5034983c10423f800bbc2661741f39e43ab8c8d
- a3cd781b14d75de94e5263ce37a572cdf5fe5013ec85ff8daeee3783ff95b073
- 686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424
- 1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126
- 59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c
- 59cd62ad204e536b178db3e2ea10b36c782be4aa4849c10eef8484433a524297
- 3ce48f371129a086935b031333387ea73282bda5f22ff78c85ee7f0f5e4625fe
- ea52d6358d53fc79e1ab61f64cb77bb47f773f0aa29223b115811e2f339e85f5

DOMAINS

1. syncronize.3utilities[.]com
2. msoffice.user-assist.site
3. userveblog.ddns[.]net
4. 151.80.14[.]194
5. adhath-learning[.]com
6. stepontheroof[.]com
7. ns1[.]b3autybab3s[.]com
8. stilletowheels[.]com
9. b3autybab3s[.]com
10. fierybarrels[.]com
11. mail[.]cooperednews[.]info
12. ns2[.]cooperednews[.]info
13. teensechs[.]com
14. newstodayreviews[.]com
15. ns2[.]softwares-free[.]com
16. www[.]fierybarrels[.]com
17. ns1[.]cooperednews[.]info
18. znaniye-onlayn[.]com
19. cooperednews[.]info
20. nophoz[.]com
21. msoffice[.]user-assist[.]site
22. recent[.]wordupdate[.]com

VII. REFERENCES

- https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html
- https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/
- https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/
- https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat