



Active Campaign Targeting Middle East

CRITICALITY



23/01/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

An active campaign targeting Middle East and Africa through Middle Eastern geopolitical-themed lures to distribute a Remote Access Trojan (RAT).



Threat Details

An active campaign targeting Middle East and Africa through Middle Eastern geopolitical-themed lures. In this campaign, the Earth Bogle threat actor uses public cloud storage services files.fm and failiem.lv to host and distribute the NjRAT malware on the web servers.

The NjRAT also known as Bladabindi is a Remote Access Trojan (RAT) malware. It is mostly used to gain unauthorized access and control over the infected machines such as stealing sensitive information, taking screenshots, getting a reverse shell, process, registry and file manipulation, uploading/downloading files, and performing other operations. The malware distributed via social media (Facebook and Discord appear to be favoured among these campaigns), file sharing (OneDrive), or a phishing email.

As observed, the Microsoft Cabinet (CAB) hides the malicious file under an audio file leveraging the geopolitical theme as a lure to entice Arabic speakers into opening it, the file contains a Virtual Basic Script (VBS) dropper masquerading as an image file fetches the malware and retrieves a PowerShell script responsible for injecting NjRAT into the compromised victim's machine. The PowerShell script drops five files: two binaries, a VBS script, a PowerShell script, and a Windows batch script. Each file has specific functionality, the Payload_1: Process injector, the Payload_2: NjRAT, the gJhkEJwBCHe.vbs: Executes rYFFCeKHIIT.bat, the rYFFCeKHIIT.bat: Executes KxFXQGVbtb.ps1, and the KxFXQGVbtb.ps1: Load Payload_1 and Payload_2 into the memory and inject NjRAT into the aspnet_compiler.exe via payload_1.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

Peter Girnus, A. Z. (2023, January). *Earth Bogle: Campaigns Target the Middle East with Geopolitical Lures*. Retrieved from Trend Micro:
https://www.trendmicro.com/en_us/research/23/a/earth-bogle-campaigns-target-middle-east-with-geopolitical-lures.html



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Center recommends all the entities to follow the below steps:

- Ensure that all your systems have endpoint protection software installed and up to date.
- Ensure that all your systems are up to date.
- Ensure that all cloud infrastructures properly secured.
- Regularly run vulnerability assessments on your internet facing systems.
- Regularly review your systems, especially internet facing systems, for misconfigurations
- Use strong passwords and Two Factor Authentication (2FA).
- Remaining vigilant against phishing attacks and sceptical regarding sensational topics and themes abused online as lures.
- Users should be wary of opening suspicious archive files such as CAB files, especially from public sources.
- Consider multi-layered defensive strategy that can detect, scan, and block malicious URLs.



Appendix B – Indicators of Compromise

Type	Value
Filename	Recording voice Qatar - Turkey.vbs UAE Embassy to Israel - Documents 2022.vbs Documents Libya Israel - 2023.vbs Israel and the UAE 2022.vbs Libya recording voice - 2023.vbs Voice Libya recording Hafter - 2022.vbs Voice of Israel and the UAE - 2022.vbs Qatar and Libya documents 2022.vbs List of names Qatar 2022.vbs gJhkEJvwBCHe.vbs_ Audio recording of Libya and the Emirates.vbs 555555555555555555555555(OUT).jpg DFvKKnFBvI_HEX.jpg FdysGNjmSf_DEC.jpg 10.jpg rYFFCeKHlIT.bat_ payload1.exe_ payload2.exe_
Hashes	2f1c9ae4477f2b990ec6d084cb00c791b4e33be4828bda947f6c600239a13d0a 6bd72e80361c1be1a3cbe79f26d34855a0fd6483784b0de5f30bf36b4536a9c1 a531b9fdb6c216839451aae63cd2a13e552ac1960ae3f2e298a1c8fca54b96c3 9c2f26dcba299e0fadd6c400adc4cef030fb5b66c10cceccf2f99849871f5490 d039aebefb27b463d620f462938ade04c0492f5274d0b28a44777e6de4c80673 00d8ac438ea309ca28693b9760bf9c2a6dce079699c503f7d7ba749fdbc8f4c1 f17059c48b1f2a9f80eae8dca222d5753aa3d8d20a26bf67546a084ca79e108e 74aad1d1c94d222b5ab92efd6c7aaf1b40c3246a44917a51d6bf6f45d6f9a65b 4888c4fe2e334dcb358ca810229f1d0699c792cf8b6fbf2e1b48a66f7b2d695c 353e4e1f3e4002e3d4264ac3ede26991cf5dcbe24774e9c1eb6e2a6e2d730778 6560ef1253f239a398cc5ab237271bddd35b4aa18078ad253fd7964e154a2580 9bb8f517fd031f9c839cd54d8b6c04fb51768d778e0f640619b019d3ba1f7f55 78ac9da347d13a9cf07d661cdcd10cb2ca1b11198e4618eb263aec84be32e9c8 67c4f872bff257417a98a8bb75ac110d3ca5c7d5584f2de3c5a2337d2a948710 c03299acd37ab7c15f0d949d15f38cceacbf817106382616e6d4064a2315942 60eeb78b09fc7fe64dde782609edc2ab4eb6daff3df1db88b054932f417e5b45 8ecc313c38eae8fa61c67bbe37532022b6deff76ae857961fc594190cff2f7a7 be979023ad6ab5427be284eac89929a9ce1d2fb83d6e28f7ce1748a4f3756e49 4c24d601bda43317eded06b0aad61fb6734e760048193779006a1030d39f5a4a af1f23e8fbc2c39e30644bb6715dd272c4b237974124f4425ab4d90fb7b4c087
Domains	gpla[.]gov[.]ly 2525[.]libya2020[.]com[.]ly
URLs	https[:]//fv9-2[.]failiem[.]lv/f/nvge8wkk3 https[:]//fv9-2[.]failiem[.]lv/down[.]php?i=nvge8wkk3 https[:]//gpla[.]gov[.]ly/out/555555555555555555555555(OUT)[.]jpg https[:]//gpla[.]gov[.]ly/4444488888/DFvKKnFBvI_HEX[.]jpg https[:]//www[.]gpla[.]gov.ly/news/ETErpTJVDq_DEC[.]jpg https[:]//gpla[.]gov[.]ly/333333/cEsITGEhOH_aaaaaa[.]jpg https[:]//www[.]shorturl[.]at/fkvxD



	https://cdn[.]discordapp[.]com/attachments/1003201277469138987/1003219218424135680/456456465[.]jpg https://onedrive[.]live[.]com/download?cid=FFEE38EB861E9448&resid=FFEE38EB861E9448%211405&authkey=AOJ0s9tYFj7d0kg
--	--



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following best security practices.

- Backup daily important new/changed data, software and configuration settings, store disconnected data retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts to read emails or to browse the web.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
[http://www.asd.gov.au/publications/protect/Microsoft Office Macro Security.pdf](http://www.asd.gov.au/publications/protect/Microsoft%20Office%20Macro%20Security.pdf)
- Whitelist applications of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- Harden user application. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Activate multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls while prioritizing the implementation of the top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement strategies to mitigate cyber security incidents. (<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Use network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Use The host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Use endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free Symon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Detect and response to incidents continuously with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - Refer to MITRE Corporation which provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction