



OilRig Targeting Middle East with New Backdoor

CRITICALITY



7/02/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A cyber espionage campaign by an Iranian nation-state Advanced Persistent Threat (APT) targeting government organizations in the Middle East through a new strain of malware.



Threat Details

An Iranian Advanced Persistent Threat (APT) OilRig has been targeting government organizations in the Middle East through a new backdoor. OilRig is highly suspected of its association with APT34, Cobalt Gypsy, Europium, and Helix Kitten cyber-espionage groups. The main purpose of this campaign is to gain access to corporate networks and exfiltrate sensitive data.

The threat actor distributed phishing emails to the victims through the government's Exchange Servers from legitimate compromised valid accounts with stolen passwords. The attack begins with a .NET-based dropper responsible for delivering four different files including one main implant called "DevicesSrv.exe" used to exfiltrate the desired data. As observed, the .NET backdoor uses the stolen credentials to send electronic missives to actor-controlled email Gmail and Proton Mail addresses. Moreover, a Dynamic-Link Library (DLL) file is used to harvest domain users and local account credentials.



Recommendations



Prevention

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

References

Lakshmanan, R. (2023, February 03). *Iranian OilRig Hackers Using New Backdoor to Exfiltrate Data from Govt. Organizations*. Retrieved from The Hacker News:
<https://thehackernews.com/2023/02/iranian-oilrig-hackers-using-new.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:

- Be wary of emails that ask for personal information. Legitimate companies will never ask for sensitive information such as passwords or credit card numbers via email.
- Look out for misspellings and poor grammar in the email body. Phishing emails often contain typos and other errors that legitimate companies would not make.
- Do not click on any links or attachments in suspicious emails. Hover your mouse over any links to see where they are actually linking to before clicking on them.
- Use endpoint protection a spam filter to help protect your computer from malicious software and phishing attempts.
- Use strong passwords and Two Factor Authentication (2FA).
- Consider multi-layered defensive strategy that can detect, scan, and block malicious content.



Appendix B – 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 C – 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