



Destructive Attacks by MuddyWater and DEV-1084

CRITICALITY



10/04/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

An Iranian nation-state Advanced Persistent Threat (APT) MuddyWater in partnership with DEV-1084 has been observed conducting destructive attacks on hybrid environments targeting Middle East.



Threat Details

An Iranian Advanced Persistent Threat (APT) MuddyWater in partnership with DEV-1084 has been observed conducting destructive attacks on on-premises and cloud infrastructures targeting Middle East. The shared characteristics between these Iranian threat actors are that they have common purposes including espionage, intellectual theft, and destructive or disruptive operations.

MuddyWater is an Iranian Advanced Persistent Threat (APT) that has been active since at least 2017. It is highly suspected of its association with Boggy Serpens, Cobalt Ulster, Earth Vetala, ITG17, Mercury, Seedworm, Static Kitten, TEMP.Zagros, and Yellow Nix. While DEV-1084 is highly suspected of its association with "DarkBit".

MuddyWater can be described as a "conglomerate" including several smaller clusters, and DEV-1084 could be considered a node of one of these clusters. However, there is no evidence to indicate if DEV-1084 operates independently or collaboratively with MuddyWater or another Iranian threat actor, or if it is a sub-team that demanded when there is only a destructive attack. As observed, both Mercury and DEV-1084 are associated with the same infrastructure, IP address, and tooling overlaps. Moreover, a reverse tunneling utility called "Ligolo" was used, and it is a MuddyWater artifact.

The attack starts when MuddyWater gains initial access to the target environment by exploiting known unpatched vulnerabilities consequently the DEV-1084 conducts destructive actions such as performing extensive reconnaissance and discovery, establishing persistence, and moving laterally throughout the network. DEV-1084 relay on compromised credentials to escalate the privileges to perform encryption of on-premises devices and large-scale deletion of cloud resources, including server farms, virtual machines, storage accounts, and virtual networks.

Through Exchange Web Services, threat actors can acquire complete access to email inboxes, doing thousands of search activities and impersonating an anonymous high-ranking employee to send messages to both internal and external recipients. The attack duration is estimated to be roughly 3h time frame starting with logging into the Microsoft Azure environment using the compromised credentials and ended when the attacker sent emails to other parties after the successful cloud disruption.



Recommendations



Prevention

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

References

Lakshmanan, R. (2023, April 8). *Iran-Based Hackers Caught Carrying Out Destructive Attacks Under Ransomware Guise*. Retrieved from The Hacker News :
<https://thehackernews.com/2023/04/iran-based-hackers-caught-carrying-out.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.
- Regularly run vulnerability assessments.
- Regularly review for misconfigurations such as:
 - Make sure that accounts do not use the default password.
 - Ensure that all server components are up to date.
 - Ensure that services are running using service accounts. Never run services using administrator accounts.
- Ensure backup of important data.
- Remove the default admin user.
- Use strong passwords and Two Factor Authentication (2FA).
- Periodically review users' permissions.
- Implement the principle of least privilege.
- Implement network segmentation.
- Limit login attempts.
- Regular security audits are important to identify vulnerabilities in the environment and to ensure that security measures are up to date.
- Keeping software up to date is important to prevent vulnerabilities that can be exploited by attackers.
- Employees should be trained on how to recognize and report suspicious activity.



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