



New Threat Actor Targeting Middle East

CRITICALITY 

27/09/2022

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A recent discovered threat actor that known as 'Metador' targeting telecommunications, Internet Services Providers (ISPs), and universities in both Middle East and Africa.



Threat Details

Metador is a recent advanced threat actor that is targeting organizations in Middle East and Africa through two complex Windows-based malwares 'metaMain' and 'Mafalda' which loaded in the memory by utilizing "cdb.exe" Windows debugging tool. The use of attack infrastructure Living-off-the Land Binary (LoLBins) to decrypt and load a malware that runs entirely in memory and leaving no unencrypted trace with using a single IP address per victim allow the threat actor to stay hidden on victim networks and accomplish long-term persistence without raising the suspicion of a compromise.

According to the researchers, Mafalda is difficult to analyze in detail as it is multi-layered obfuscation. As documented, a dedicated team develops the malware, and different team operating it, this framework accepts up to 67 commands including file operations, reading directories contents, manipulate the registry, reconnaissance of the network and the system, and exfiltrating data to the Command and Control (C2) server. While metaMain is utilized for hands-on operations, such as taking screenshots, performing file actions, logging keyboard events, and supports arbitrary shellcode execution. On the other hand, analysts found 'Cryshell' which used for internal network bouncing besides of other indicators belong to unnamed Linux tool that steals data from workstations and channels them back to Mafalda.

As observed by researchers, Metador developers are well-resourced group able to improve the tools due to the complexity of the malware. Besides, some of the members are fluent in English. However, others are non-native English speakers as Spanish language was present in Mafalda code. Researchers believe that behind Metador is "a high-end contractor arrangement," like one typical for a nation-state operation.



Recommendations



Prevention

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

References

Staff, I. W. (2022, September 26). *Researchers discover new hacker group “Metador”*. Retrieved from IT World Canada : <https://www.itworldcanada.com/post/researchers-discover-new-hacker-group-metador>

Toulas, B. (2022, September 25). *New hacking group ‘Metador’ lurking in ISP networks for months*. Retrieved from Bleeping Computer: <https://www.bleepingcomputer.com/news/security/new-hacking-group-metador-lurking-in-isp-networks-for-months/>



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 follow these steps:

- Educate users on malware threats—train your users on techniques that can help them avoid social engineering schemes, such as phishing attacks, and report suspicious communication or system behavior to the security team.
- Strong passwords and software updates—ensure all users create strong, unique passwords, and regularly change passwords. Use a password manager to make it easier for users to use and remember secure passwords. Update your systems as quickly, as security flaws become known and patches are released.
- Back up your data and your test restore procedures—backup is a critical practice that can help to protect against data loss. It can help ensure that normal operations can be maintained even if the organization is attacked by network-based ransomware worms or other destructive cyber attacks.
- Partition your network—you should use network segmentation to isolate important parts of your network from each other. This can significantly reduce the “blast radius” of successful attacks, because attackers will be limited to a specific network segment and cannot move laterally to other parts of the network.
- Implement a layered security approach, including a secure email solution, a company-sanctioned file-sharing solution, and endpoint protection on user devices.
- Continuously monitor network traffic.
- Deploy a zero-trust security framework.



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**Not for disclosure, restricted to participants only.**

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

AMBER**Limited disclosure, restricted to participants' organizations.**

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. *Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.*

GREEN**Limited disclosure, restricted to the community.**

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

WHITE**Disclosure is not limited.**

Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.