



TA402 Targeting Middle East Government

CRITICALITY

16/11/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A phishing campaign is targeting government entities in the Middle East. This campaign utilizes a new malware variant known as IronWind to deliver malicious payloads.



Threat Details

Proofpoint has reported that a threat actor known as TA402 is actively targeting government entities in the Middle East. The threat actor uses a new malware called IronWind to deliver malicious payloads.

IronWind is a multi-stage malware characterized by its utilization of various techniques to evade detection. In its initial stage, the malware functions as a downloader, retrieving the second stage from a remote server. The second stage serves as a dropper responsible for installing the third stage, which constitutes the payload. This payload operates as a backdoor, enabling remote control of the infected system by the threat actor.

In their recent campaigns, TA402 has been utilizing a compromised Ministry of Foreign Affairs email account to distribute phishing emails containing Dropbox links that lead to the deployment of IronWind malware.



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

New Campaign Targets Middle East Governments with IronWind Malware. (2023). Retrieved from TheHackerNews: <https://thehackernews.com/2023/11/new-campaign-targets-middle-east.html>

TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities . (2023). Retrieved from Proofpoint: <https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to apply the following steps:

- Implement a strong email security solution that can block phishing emails.
- Educate employees about phishing attacks and how to spot them.
- Keep software up to date, including security patches.
- Use a strong password policy and require multi-factor authentication.



Appendix B – Indicator of Compromise

Type	Value
IP Addresses	191[.]101.78[.]189
SHA256	9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47 5d773e734290b93649a41ccda63772560b4fa25ba715b17df7b9f18883679160 19f452239dadcd7544f055d26199cb482c1f6ae5486309bde1526174e926146a - A4bf96aee6284effb4c4fe0ccfee7b32d497e45408e253fb8e1199454e5c65a3 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47 - cbb89aac5a2c93a02305846f9353b013e6703813d4b6baff8eb89ee938647af3 - c98dc0b930ea67992921d9f0848713deaa5bba8b4ba21effd0b00595dd9ed28c - ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368 - e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c - d8cde28cf2a5884daddf6e3bc26c80f66bc3737e426b4ba747d49d154999fbc1 81fc4a5b1d22efba961baa695aa53201397505e2a6024743ed58da7bf0b4a97f 3b2a6c7a39f49e790286185f2d078e17844df1349b713f278ecef1defb4d6b04 7bddde9708118f709b063da526640a4132718d3d638505aafce5a20d404b2761 883e035f893483b9921d054b3fa014cef90d90b10dcba7d342def8be2e98ce3c 4b0a48d698240504c4ff6275dc735c8162e57f92224fb1d2d6393890b82a4206 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115 3d80ea70b0c00d12f2ba2c7b1541f7d0f80005a38a173e6962b24f01d4a2a1de
Domains	- inclusive-economy[.]com - healthcaption[.]com - theconomics[.]net



Appendix C – Best Practices

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

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, 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 for reading email and web browsing.
- 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
- Application whitelisting 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.
- User application hardening. 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.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and 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:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon 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.
- Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
- MITRE Corporation 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