



WIRTE Campaign Targets Middle East Entities

CRITICALITY 

01/12/2021

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A threat group known as WIRTE targets several entities in the Middle East by sending phishing emails containing malicious Excel/Word documents.



Threat Details

A government-targeting campaign known as WIRTE is targeting diplomatic, financial institutions, government, law firms, military organizations, and technology companies. The targeted countries are Armenia, Cyprus, Egypt, Jordan, Lebanon, Palestine, Syria, and Turkey.

For gaining an initial foothold, the threat actor sends phishing emails with malicious Microsoft Office Word and Excel documents. The Excel droppers use Excel 4.0 macros to download and install the next-stage implant by running multiple formulas in a hidden column to hide the enable editing button and unhide the spreadsheet that contains decoy. One of the formulas will get the name of the environment, check if a mouse is present, and check if the host computer can play sound. If all checks are met, a VBS script that capable to write an embedded PowerShell snippet will be generated by the macro to download payloads and receive commands from the C2. Cloudflare has been used to disguise the IP addresses of the threat actors' C2 domains.

As observed by kaspersky, the threat actor used several commands to list local disk drives, get list of installed AV software, check whether the user is admin or not, check if any backdoor services are available, check for registry keys that have been added to enable COM hijacking, list all of the hotfixes that have been installed and take a screenshot and save it to %AppData% till the next POST request. Despite the group's apparent lack of sophistication, the company warns that these actors' TTPs are nevertheless very efficient in attacking the group's targets.



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

Stealthy WIRTE hackers target governments in the Middle East. (2021). Retrieved from BleepingComputer: <https://www.bleepingcomputer.com/news/security/stealthy-wirte-hackers-target-governments-in-the-middle-east/>

WIRTE Hacker Group Targets Government, Law, Financial Entities in Middle East. (2021). Retrieved from The Hacker News: <https://thehackernews.com/2021/11/wirte-hacker-group-targets-government.html>

WIRTE's campaign in the Middle East 'living off the land' since at least 2019. (2021). Retrieved from SecureList: <https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044/>



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 follow the below steps:

- Email content filtering. Whitelist allowed attachment types (including archives and nested archives). Analyse/sanitize hyperlinks, PDF, and Microsoft Office attachments. Quarantine Microsoft Office macros.
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads, and Java on the Internet.
- Web content filtering. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks, and free domains.
- Protect your workstations and servers. We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates, and installing antivirus software.



Appendix B – Indicators of Compromise

Indicators of Compromise

Malware URLs

nutrition-information[.]org
Stgeorgebankers[.]com
Firstohiobank[.]com
allaccounting[.]ca
est-clinic[.]com
unitedfamilyhealth[.]net
pocket-property[.]com
kneeexercises[.]net
doctoressolis[.]com
omegaeyehospital[.]com
Healthyhabitsusa[.]com
niftybuysellchart[.]com
Dentalmatrix[.]net

File names and Hashes

ecaaab9e2fc089eefb6acc	
ae9750ac60	اللائحة الجنيسية.xls
a7802c9a4046edbcbe3f5	
a503de61867	تعميم رقم-1803202155.doc
3a7425539f8853e7b896	saint george bankers & trust business
24890a5de25b	offer.docx
5AE4505A5CA7235C842	
680C557D05383	slmgr.vbs
B2F8CCE7B03E7AA70DA	
B4A5D377375B5	exhaustedq.txt
8ade05c4b4e98cc89fa09	
bd513ea1a99	kaspersky update agent.exe

IP addresses

91.211.89[.]33
91.203.6[.]27
45.129.96[.]174
45.129.97[.]207

Please find the list of full IOCs in the attached Excel document.



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

TLP: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.

TLP: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.**

TLP: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.

TLP: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.