



TA402 Attacks Governments in The Middle East

CRITICALITY

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

A threat group known as TA402 is targeting government institutions in the Middle East by sending malicious emails.



Threat Details

TA402 is a Palestinian threat group that targets the Middle East. The activity of TA402 based on sending emails containing either malicious links or PDF attachments in the Arabic language, the content of the email is usually related to geopolitical situations in the Middle East, such as "A delegation from Hamas meets with the Syrian regime" and "Hamas member list".

For the initial access, the attacker sends an email with multiple geofenced URLs based on IP addresses; the primary purpose of the geofenced URLs is to target the computers with Arabic language packs installed then download password protected RAR files that contain the malware; the reason behind the password-protected files is to avoid automated threat analysis. However, the non-targeted recipients of the group will be diverted to legitimate websites. The PDF attachment contains the archive file password. Extracting the archive file drops a malware called LastConn.

LastConn is a backdoor that allows the threat actors to run arbitrary commands and takes screenshots, then exfiltrate them via Dropbox. LastConn can also prevent both automated and manual malware analysis.



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

Molerats APT renews phishing attack against Middle Eastern governments. (2021). Retrieved from CIO: <https://www.cio.com/article/3622456/molerats-apt-renews-phishing-attack-against-middle-eastern-governments.html>

Molerats Hackers Actively Targeting Middle East Governments. (2021). Retrieved from CYWARE SOCIAL: <https://cyware.com/news/molerats-hackers-actively-targeting-middle-east-governments-ec4c1cd2>

New TA402 Molerats Malware Targets Governments in the Middle East. (2021). Retrieved from Proofpoint: <https://www.proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-middle-east>

The return of TA402 Molerats APT after a short pause. (2021). Retrieved from Security Affairs: <https://securityaffairs.co/wordpress/119085/apt/ta402-molerats-apt-return.html>



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 to help organizations thwart these attacks:

- Verify the target sites SSL credentials.
- Watch out for shortened links.
- Be wary of Suspicious Attachments.
- Never click on hyperlinks in email.



Appendix B – Indicators of Compromise

Indicators of Compromise

Malware URLs

hxxps://script[.]google[.]com/macros/s/AKfycbXhRyJqO682mzT4C3-aNwSULjNPuHvhqpGYEIJedUBPfaG60fZSOEQ/exec

hxxps://justpaste[.]it/ONE_ME_OR18

hxxps://pastebin[.]com/raw/q81XevX2

hxxp://192[.]210[.]151[.]43/CVDWwr42525[.]php

File names and Hashes

إجتماع وفد من حماس مع النظام السوري.exe

SHA-256 f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45

Viewfile.exe

SHA-256 f55e2050733576fa16452e2589a187f4bf202ca3b54b1497ba2c006e8d3bdd45

ViewfileQA.exe

SHA-256 0f36088ed9f5ffd4b42d35789113e99d8839edc52e554dbee0969bcad0200cfb

Hamas-Syria.rar

SHA-256 0db46fea5a0be8624069f978f115e4270833df29ed776c712182327a758fd639

hamas - syria.pdf

SHA-256 557c60ae9c613164fda3189720eaf78fe60b6bd8191f4d208ca3bbbdceffee36

Hammas.exe

SHA-256 1cf18ce4becf2244fb715aa52eb4d56b569a95f2a1e7a835d217a20a2757a2d8

Hammas.exe

SHA-256 6d65804ca8f71e21b18de08176a53d8f203bc23629dd822ef3c0da217f95f119

Hammas.rar

SHA-256 cd60488acc0cc596c0de63eb0a7bca4ada4748fc4e76a86ca0fab42f15050347



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.