



A New Phishing Campaign By MuddyWater

CRITICALITY



11/12/2022

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

MuddyWater a sponsored nation state Iranian threat actor, utilized compromised email accounts to deliver phishing emails to their targets. Observed targets were two Egyptian hosting companies, and multiple insurance companies in Israel.



Threat Details

MuddyWater leveraged a remote administration tool (Syncro), that is designed for managed service providers (MSPs). The group targeted two Egyptian hosting companies, one was compromised to spread the phishing emails, the other was the recipient of the malicious message.

The initial infection vector is phishing sent from a compromised legitimate business email account, although the official signature of the company was missing targets still trusted the email considering that it came from a legitimate business email address. To evade detection the threat actors attached an HTML file containing the URL to download the Syncro MSI installer.

It was observed that most Syncro installers were hosted on OneHub cloud storage, a service that the actor has used in previous campaigns. Once Syncro is installed on the target system, backdoors are deployed to gain persistence and exfiltrate data.

MuddyWater tactics are not immensely sophisticated, yet it has been observed that the group mainly used freely available tools for its operations.



Recommendations



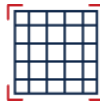
Prevention

- **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.



MITRE ATT&CK

- **Appendix C** contains the Mitre ATT&CK details.

References

Ilascu, I. (2022, December 8). Hacked corporate email accounts used to send MSP Remote Access Tool. BleepingComputer. Retrieved December 11, 2022, from <https://www.bleepingcomputer.com/news/security/hacked-corporate-email-accounts-used-to-send-msp-remote-access-tool/>

New Muddywater Threat: Old Kitten; new tricks. Deep Instinct. (2022, December 8). Retrieved December 11, 2022, from <https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks>



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 monitor for remote desktop solutions that are abnormal in the organization.



Appendix B – Indicators of Compromise

Hashes

f511bdd471096fc81dc8dad6806624a73837710f99b76b69c6501cb90e37c311
efd5271bdb57f52b4852bfda05122b9ff85991c0600befcbd045f81d7a78eac5
d65d80ab0ccdc7ff0a72e71104de2b4c289c02348816dce9996ba3e2a4c1dd62
1670a59f573037142f417fb8c448a9022c8d31a6b2bf93ad77a9db2924b502af
dedc593acc72c352feef4cc2b051001bfe22a79a3a7852f0daf95e2d10e58b84
eae0acba9c9e6a93ce2d5b30a5f21515e8ccca0975fbd0e7d8862964fdfa1468
7e7292b5029882602fe31f15e25b5c59e01277abaab86b29843ded4aa0dcbdd1
c7a2a9e020b4bcbfa53b37dea7ebf6943af203b94c24a35c098b774f79d532ac
887c09e24923258e2e2c28f369fba3e44e52ce8a603fa3aee8c3fb0f1ca660e1
01dfa94e11b60f92449445a9660843f7bea0d6aad62f1c339e88252008e3b494
d550f0f9c4554e63b6e6d0a95a20a16abe44fa6f0de62b6615b5fdcdb82fe8e1
61dcf1eeb616104742dd892b89365751df9bb8c5b6a2b4080ac7cf34294d7675
c6cfd23282c9ff9d0d4c72ee13797a898b01cd5fd256d347e399e7528dad3bfd
5578b7d126ebae78635613685d0cd07f4fb86f2e5b08e799bdc67d6d6053ede2
32339f7ac043042e6361225b594047dd4398da489a2af17a9f74a51593b14951
dab77aea8bf4f78628dcf45be6e2e79440c38a86e830846ec2bddc74ff0a36e4
b5c7acf08d3fd68ddc92169d23709e36e45cb65689880e30cb8f376b5c91be57
2a5f74e8268ad2d38c18f57a19d723b72b2dadd11b3ab993507dd2863d18008d
e87fe81352ebda0cfc0ae785ebfc51a8965917235ee5d6dc6ca6b730eda494cf
aa282daa9da3d6fc2dc6d54d453f4c23b746ada5b295472e7883ee6e6353b671
4e80bd62d02f312b06a0c96e1b5d1c6fd5a8af4e051f3f7f90e2976580842515
697580cf4266fa7d50fd5f690eee1f3033d3a706eb61fc1fca25471dbc36e684
dc7e102a2c68f7e3e15908eb6174548ce3d13a94caadf76e1a4ee834dc17a271
f24ce8e6679893049ce4e5a03bc2d8c7e44bf5b918bf8bf1c2e45c5de4d11e56
433b47f40f47bea0889423ab96deb1776f47e9faa946e7c5089494ed00c6cc29
011cb37733cdf01c689d12fedc4a3eda8b0f6c4dcdeef1719004c32ee331198e
e217c48c435a04855cf0c439259a95392122064002d4881cf093cc59f813aba8
331b513cf17568329c7d5f1bac1d14f38c77f8d4adba40c48dab6baf98854f92
4d24b326d0335e122c7f6adaa22e8237895bdf4c6d85863cf8e84cfcc0503e69
a35a1c92c001b59605efd318655d912f2bcd4e745da2b4a1e385d289e12ee905
4550b4fa89ff70d8ea59d350ad8fc537ceaad13779877f2761d91d69a2c445b2
653046fa62d3c9325dbff5cb7961965a8bf5f96fa4e815b494c8d3e165b9c94a
76ab046de18e20fd5cddb90678389001361a430a0dc6297363ff10efbcb0fa8

**Appendix C – MITRE ATT&CK**

Tactic	Technique
Initial Access	T1566.001 Phishing: Spearphishing Attachment
	T1566.002 Phishing: Spearphishing Link
Resource	Acquire Infrastructure: Web Services – T583.006
Development	Compromise Accounts: Email Accounts– T1586.002
Command and Control	T1219 Remote Access Software
Resource	T1588.002 Obtain Capabilities: Tool
Development	T1583.006Acquire Infrastructure: Web Services



Appendix D – Best Practices

Bahrain National CERT team recommends organizations 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 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 with 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 centralized time-synchronized 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 E – 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