



## MalKamak Targets Global Aerospace & Telecoms Firms

CRITICALITY 

12/10/2021

### Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

### Summary

A new Iranian threat actor named “MalKamak” conducted “Operation GhostShell” by utilizing ShellClient RAT to target **the aerospace and telecommunications industries in the U.S., Russia, Europe, but mainly in the Middle East.**



## Threat Details

Cybereason company reports about a recent cyber-espionage campaign by a new Iranian threat actor named "Malkamak" that is targeting the aerospace and telecommunications industries notably in the Middle East.

The Operation Ghostshell attacks indicate utilization of the ShellClient RAT the Remote Access Trojan, and after investigations, the Nocturnus team noticed hidden persistent developments of ShellClient RAT at least since November 2018. Initially, the operation was about a standalone reverse shell, until becomes an advanced backdoor by adding multiple iterations on the malware to establish new functionalities; therefore, the adversary executes malicious binary to perform credential dumping.

The ShellClient RAT was built to control fingerprinting and registry operations. Also, it uses Dropbox cloud storage for command-and-control (C2) communications. To evade security solutions, the DropBoxC2 tool encrypts traffic, which makes the network traffic appear legitimate. The Dropbox storage possesses three folders, one for each infected system, one for the ShellClient RAT's commands, and one for the outcomes of those commands, consequently, the victim machine checks the commands folder every two seconds, finds files that represent commands, parses their content, deletes them from the remote folder, and allows them to be executed.

While still in speculation "Malkamak" was observed to have connections with other Iranian State-sponsored actors such as Chafer APT and Agrius APT as well as chinese threat actor "IndigoZebra" that is known for storing commands via Dropbox API.

*Indicators of compromise (IOC) are in the Appendix B section of this document.*

*Mitre ATT&Ck table is in the Appendix C section of this document.*



## 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

CybereasonNocturnus. (2021, October 6). *Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms*. Retrieved from cybereason:  
<https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms>

Lakshmanan, R. (2021, October 6). *Iranian Hackers Abuse Dropbox in Cyberattacks Against Aerospace and Telecom Firms*. Retrieved from The Hacker News:  
<https://thehackernews.com/2021/10/iranian-hackers-abuse-dropbox-in.html>

mohdrennis. (2021, October 6). *Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firm*. Retrieved from alienvault:  
<https://otx.alienvault.com/pulse/615dbbe5c465a27aa4da6241>



## Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: [CERT@ncsc.gov.bh](mailto: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). Analyze/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 – Detection

### Indicators of Compromise

#### #Hashes

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SHA-1</b>   | 4f0ffee3bed7a6dd31f1d1dd17f73045b6b4fdec<br>5bf29e7c3b1e3c6743af039689da102f0f877a9f<br>6f81ccb61dcd79cc5fd23c2b6289c2350eee7c36<br>b5ea3a577a1b39458d8f493abdc14c406abaca96                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>MD5</b>     | 1f52b1901edcfff20e2fb436057a27b2<br>370050d967040f4a4b0dd71bee533089<br>57f4c3daa3fb6c5155cb40c60d634688<br>7cba41b2cab8e8a263167dacc5dc96eb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>SHA-256</b> | 186ab2a5662c5e3994ee1cbfcf9e7842f1e41b1a4041c67f808914dfc8850706<br>19e040305fb57592bb62b41c24e9b64162e1e082230a356a304a3193743b102d<br>21cc9c0ae5f97b66d69f1ff99a4fed264551edfe0a5ce8d5449942bf8f0aefb2<br>2a1044e9e6e87a032f80c6d9ea6ae61bbb053c0a21b186ecb3b812b49eb03b7<br>49c41771e8e348b30de43d1112221c71a6497794b541fead7f3b2eab706afba3<br>5d5ff74906d2666be0fbfe420c5d225684aa1cb516fffc32cfeee9e788e4b6e4<br>6b7b6e973779c1a07891cc1fa7b3e4078a1308c4114296eb3ea429e08793efe0<br>a541afa0e73c3942b8c3645a3ba1ea59c4d6e1110e271be34fdb6a8c02a299e2<br>d7aa669de0f8a0cdb898cf33ac38ae65461de3c8c0c313c82ee8d48e408e4c4d |

#### #IP Addresses

- 139.162.120[.]150
- 50.116.17[.]41

#### #Domains

- http://76.0[.]152[.]0
- http://azure[.]ms-tech[.]us:80
- whynooneistherefornoneofthem[.]com
- api.dropboxdapi[.]com
- azure.ms-tech[.]us



## Appendix C – MITRE ATT&CK

|                             |                                 |                                    |                                        |               |
|-----------------------------|---------------------------------|------------------------------------|----------------------------------------|---------------|
| <b>Execution</b>            | Command-line interface          | Windows Management Instrumentation | PowerShell                             |               |
| <b>Persistence</b>          | Windows Service                 |                                    |                                        |               |
| <b>Privilege Escalation</b> |                                 | Valid Accounts                     |                                        |               |
| <b>Defence Evasion</b>      | Obfuscated Files or Information | Masquerading                       |                                        |               |
| <b>Credential Access</b>    | Credential Dumping              |                                    |                                        |               |
| <b>Discovery</b>            | Security Software Discovery     | System Information Discovery       | System Network Configuration Discovery |               |
| <b>Lateral Movement</b>     | SMB/Windows Admin Shares        |                                    |                                        |               |
| <b>Collection</b>           |                                 | Archive Collected Data             |                                        |               |
| <b>Command and Control</b>  | Data Encoding                   | Encrypted Channel                  | File Transfer Protocols                | Web Protocols |
| <b>Exfiltration</b>         | Exfiltration Over Web Service   | Exfiltration Over C2 Channel       | Exfiltration Over Alternative Protocol |               |



## Appendix D – 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](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](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://attack.mitre.org/wiki/Main_Page)
    - [https://car.mitre.org/wiki/Full\\_Analytic\\_List](https://car.mitre.org/wiki/Full_Analytic_List)
    - <https://car.mitre.org/caret/#/>



## Appendix E – 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.