



Agrius Employed Wipers Disguised as Ransomware

CRITICALITY ●  —  —  —  ●

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

An Iranian threat group called Agrius hides behind ransomware to launch destructive wiper attacks against IT infrastructure targets.



Threat Details

At first sight, an investigation of a ransomware attack showed new variants of wipers used to carry out series of devastating attacks against Israeli targets related to a threat group called Agrius. Agrius does not appear to be motivated by money which is uncommon behaviour for financially motivated groups. The threat group has transformed the Apostle Wiper functionality from a wiper to fully functional ransomware and used it to target critical facilities.

For the initial access, the attacker takes advantage of an exploitable vulnerability that has been found in FortiOS known as CVE-2018-13379 and various web-based vulnerabilities to gain access anonymously to the victim's system using ProtonVPN. Once an exploit has been successful, the attacker uploads a web shell using Remote Desktop Protocol to leverage the compromised credentials and lateral movements. Moreover, the Agrius group uses the same destructive wiper malware that was linked to attacks against Saudi Arabia which is known as Deadwood.

It has also been observed that during attacks, Agrius would additionally drop a customized .NET backdoor called IPsec Helper that provides persistence and allows the system to establish a connection with a C2 (command-and-control) server (Figure: 1.1).

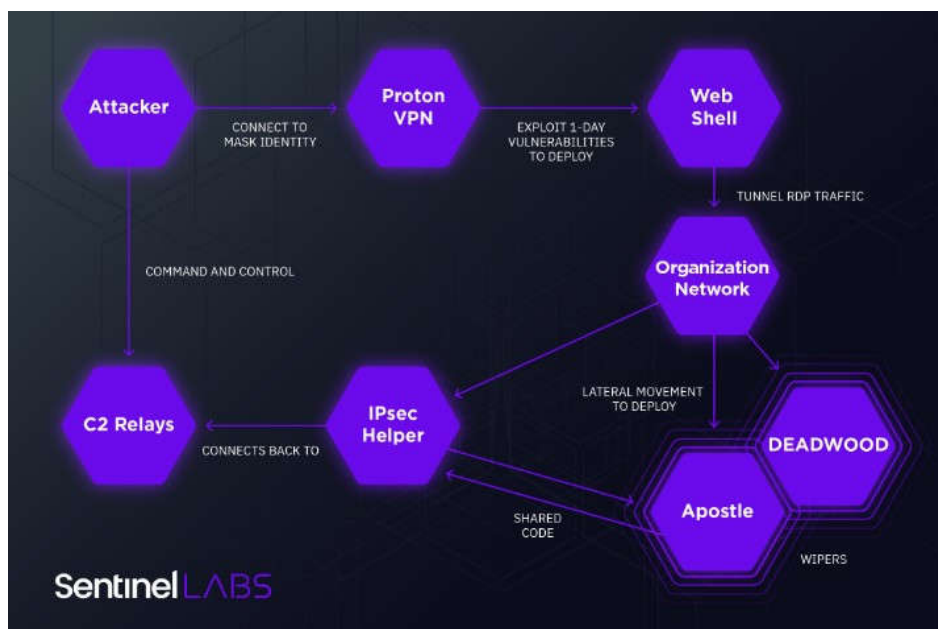


Figure 1.1: Agrius attack life cycle



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

From Wiper to Ransomware: The Evolution of Agrius. (2021, May 25). Retrieved from SentinelLabs: <https://labs.sentinelone.com/from-wiper-to-ransomware-the-evolution-of-agrius/>

Iranian hacking group Agrius pretends to encrypt files for a ransom, destroys them instead. (2021, May 25). Retrieved from ZDNet: <https://www.zdnet.com/article/iranian-hacking-group-agrius-pretends-to-encrypt-files-for-a-ransom-destroys-it-instead/>

New Iranian Group 'Agrius' Launches Destructive Cyberattacks on Israeli Targets. (2021, May 26). Retrieved from SecurityWeek: <https://www.securityweek.com/new-iranian-group-agrius-launches-destructive-cyberattacks-israeli-targets>

Threat Actor 'Agrius' Emerges to Launch Wiper Attacks Against Israeli Targets. (2021, May 25). Retrieved from Threatpost English Global threatpostcom: <https://threatpost.com/agrius-wiper-attacks-israeli-targets/166474/>



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:

- Immediately patch the vulnerability (CVEs 2018-13379).
- If FortiOS is not used by your organization, add key artifact files used by FortiOS to your organization's execution-deny list. Any attempts to install or run this program and its associated files should be prevented.
- Regularly back up data, airgap and password/protect backup copies offline.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to restore sensitive or proprietary data from physically separate hard drive.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Disable unused remote access.
- Audit user accounts with administrative privileges.
- Install and regularly update antivirus and anti-malware.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.



Appendix B – Indicators of Compromise

Indicators of Compromise

Malware URLs

hxxp://195.123.208.152/Admins/login.php
hxxp://5.2.67.85/View/list.php
hxxp://5.2.73.67/Panel/new/File/css/boot.php
hxxp://185.142.98.32/Scripts/_Data/25/lastupdate.php
hxxp://185.142.97.81/css/v1/template/main.php
hxxp://theisnonamelikethis29123.com/mail.php
hxxp://whynooneisthereforoneofthem.com/about.php

Tools

IPsec Helper
Apostle
DEADWOOD

File names

gip-starter-er-iso-sql-backup.sql-iso-9001
Microsoft.Help.dll.iso



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.