cybersecurity
associates

PowerDrop PowerShell Attack On Aerospace Industry

Threat Hunting Report

Dated: 13th July 2023

Written by: Aidan Matthews

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

Private and confidential

The information contained in this report is strictly confidential and intended solely for the use of the recipient. Any other use and any communication, publication or reproduction of the report or any portion of its contents without the written consent of the authors is strictly forbidden. The recipient agrees to indemnify and hold harmless against any damages or claims resulting from such unauthorised use.

PowerDrop PowerShell Attack On Aerospace Industry

Threat Report

Executive Summary

The purpose of this report is to document the current form and methodologies used by the PowerDrop Malware. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to detect and hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint, Microsoft Sentinel and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the lifecycle of the PowerDrop Malware and their TTPs (Tactics, Techniques and Procedures). Containing recommendations to help detect and mitigate the threat. The report also includes references where information within this report was identified from.

Tactics, Techniques & Procedures

Tactics, Techniques, and Procedures (TTPs) describes the actions, behaviours, processes and strategies used by malicious adversaries that engage in cyber-attacks.

Tactics will outline the overall goals behind an attack, including the strategies that were followed by the attacker to implement the attack. For example, the goal may be to steal credentials. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages.

Techniques will show the method that was used to engage in the attack, such as cross-site scripting (XSS), manipulation through social engineering and phishing, to name a few. Identifying the Techniques used during an attack can help discover an organisation's blind spots and implement countermeasures in advance.

Procedures will describe the tools and methods used to produce a step-by-step description of the attack. Procedures can help to create a profile for a threat actor or threat group. The analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

Analysts follow this methodology to analyse and define the TTPs to aid in counterintelligence. TTPs that are described within this research are based of the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.

Hackers

A 'hacker' is a person who finds it interesting to interfere with computer systems. Often seen as a challenge, a hacker will attempt to breach a system because it tests their skills and knowledge.

Hacktivists

A 'hacktivist' is a person who gains unauthorized access to computer files or networks in order to further social or political ends.

Insider Threats

An employee or 'insider' is a person within a group or organisation, especially someone with knowledge of information unavailable to others.

State Sponsored

A 'state actor' is a person who is acting on behalf of a governmental body and is therefore subject to regulation under their human rights.

Organised Crime

A 'criminal gang' is a group of people that take part in organised unlawful activity. They may target a business to gather information on customers or to gather financial data which could be sold.

Summary

PowerDrop is the name given to the PowerShell malware script targeting the US aerospace industry. Although it is currently unknown which individual or group is behind the attack, it is believed to be nation-state aggressors targeting the Aerospace industry due to the increased research and development in missile programs relating to the Russo-Ukraine war.

The malware was discovered and named 'PowerDrop' by Adlumin Threat Research in May 2023 and was targeting an aerospace defence contractor. This malware was detected by analysing PowerShell commands with machine learning. In order to evade detection, this malware uses evasive techniques including various forms of encoding and encryption.

Although there is existing malware with similar methods of exploiting PowerShell and WMI, PowerDrop is unique as it's code has not been used in any previous attacks and seems to be custom made to avoid detection.

MITRE ATT&CK

MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework (ATT&CK), which is used to track various techniques attackers use throughout the different stages of cyberattack to infiltrate a network and exfiltrate data.

The framework defines the following tactics that are used in a cyberattack:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

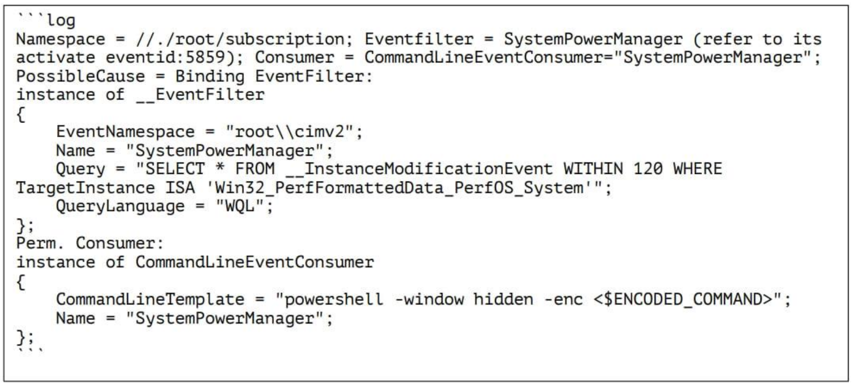
Phase 1: Initial Access: Fake Windows 10 Update

PowerDrop begins by masquerading as a legitimate Microsoft Windows 10 update to fool the victim into installing it. Furthermore, by keeping the user unaware of its true purpose, this allows the malware to further avoid detection.

Although it is still not fully understood how the malware spreads, it is suspected that the malicious individuals or group behind the attack could be using an exploit, spreading the malware via software download sites, malvertising, or potentially through phishing emails.

Phase 2: PowerShell and WMI

Once the malware has been run by the user, a PowerShell command is executed by the service WMI (Windows Management Instrumentation). The malware then creates and executes WMI event filters and consumers called 'SystemPowerManager' using 'wmic.exe' which can be seen in the image below:



~~~
```log
Namespace = //./root/subscription; Eventfilter = SystemPowerManager (refer to its
activate eventid:5859); Consumer = CommandLineEventConsumer="SystemPowerManager";
PossibleCause = Binding EventFilter:
instance of __EventFilter
{
    EventNamespace = "root\\cimv2";
    Name = "SystemPowerManager";
    Query = "SELECT * FROM __InstanceModificationEvent WITHIN 120 WHERE
TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'";
    QueryLanguage = "WQL";
};
Perm. Consumer:
instance of CommandLineEventConsumer
{
    CommandLineTemplate = "powershell -window hidden -enc <$ENCODED_COMMAND>";
    Name = "SystemPowerManager";
};
```
~~~

Figure 1: SystemPowerManager using wmic.exe

The malware is triggered by querying for updates to the class: 'WMI class Win32_PerfFormattedData_PerfOS_System' in the namespace 'root\cimv2'. Once the class is updated, the WMI event filter will trigger the PowerShell script. The purpose of 'Win32_PerfFormattedData_PerfOS_System' is to monitor Windows performance meaning that the class is updated frequently, thus making sure the script will trigger. To prevent the PowerShell script being triggered too often the query will happen once every 120 seconds; triggering the PowerShell script this way means the attacker can help maintain persistence and avoid detection.

The malware works by encoding the PowerShell arguments in Base64 and UTF-16 Little Endian to obfuscate the command line arguments, this results in a single command line argument being executed by the WMI service to avoid detection.

Cyber Kill-Chain

The cyber kill chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

This creates a backdoor or RAT (remote access trojan) providing the attackers with access to data on the affected devices remotely.

Phase 3: Remote Access

Once the malware has successfully exploited the WMI service, it now works as a remote access trojan (RAT) allowing attackers to execute code remotely on the victim device. The infected device will send an ICMP request to the command and control beacon and will wait up to 60 seconds for a response. It is believed that this will retain control of devices on high latency networks. After receiving the request from the victim device, a payload is sent from the command and control server which is encrypted by AES, then decrypted and executed once received.

Phase 4: Data Exfiltration / Remote Code Execution

Now that attackers can send commands to the victim's device, they gain unauthorised access allowing them to monitor the network, steal sensitive information and execute malicious code. Using the remote access trojan means attackers can exfiltrate financial data, intellectual property, user login credentials and more. The results of this data exfiltration can vary, from attempts to commit identity theft / fraud, blackmail or holding data for ransom.

Conclusion

Although this malware could affect anyone, companies in the aerospace industry are most at risk to it and should therefore be observant of attempts from attackers. Whilst the origin of this malware still remains undetermined, by having a high level cybersecurity posture, organisations can increase their chances of evading such attacks. Trained experts, such as those in a Security Operations Centre, can quickly spot suspicious network connections to identify and resolve a remote access incident like the one detailed above. Cyber incidents like these not only impact customers, but can result in financial losses through downtime, fines or loss of reputation.

Advice

As of now, this new malware has been spotted targeting companies in the Aerospace industry making these companies the most at risk.

Despite PowerDrop targeting the Aerospace industry, remote access trojans affect all industries and therefore all companies and individuals should ensure that they are taking the appropriate action to keep their devices and networks safe.

It is recommended to scan your system with anti-virus software continuously to detect and remove malware from your organisational devices, with automatic updates of signatures and software.

C2 servers often take advantage of vulnerabilities on the host (including browser plugins) in order to gain access, by performing vulnerability scans it's possible to detect CVE vulnerabilities and patch them before attackers can take advantage.

Organisations should also check abnormal network activity such as pinging externally. This is because the malware makes use of a remote access trojan in order to communicate with command and control servers, so by investigating the network traffic, it is possible to spot whether devices are communicating with suspicious servers.

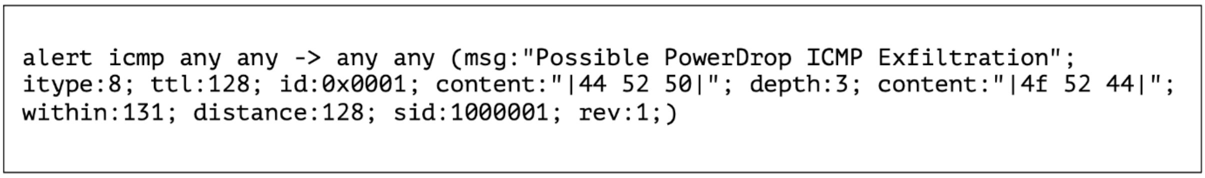
Regular Backups must be kept offline; this is the only way to protect against a determined threat actor. Also, regularly test backups for their integrity to see if they can be recovered and scan backups for registry persistence.

Detection Rules

PowerDrop malware attempts to avoid detection, but there are ways it can be detected. The following detection methods have been produced by Adlumin to help detect PowerDrop on endpoints and networks.

Snort

By running the following Snort detection rule, it is possible to detect PowerDrop malware data exfiltration in outbound traffic.

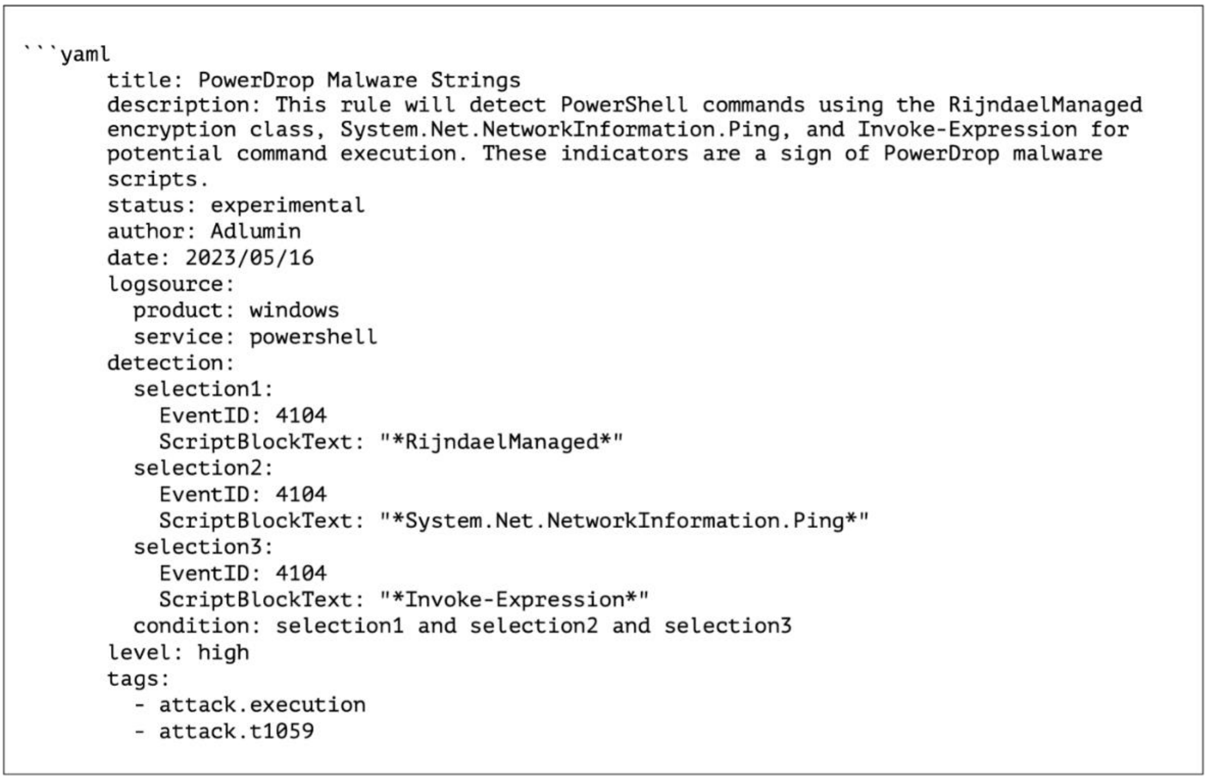


```
alert icmp any any -> any any (msg:"Possible PowerDrop ICMP Exfiltration";
itype:8; ttl:128; id:0x0001; content:"|44 52 50|"; depth:3; content:"|4f 52 44|";
within:131; distance:128; sid:1000001; rev:1;)
```

Figure 2: Snort Rule to detect outbound traffic.

SIGMA

The following SIGMA rule has been created to detect PowerDrop on an endpoint by checking for PowerShell executions used by the malware.



~~~
```yaml
      title: PowerDrop Malware Strings
      description: This rule will detect PowerShell commands using the RijndaelManaged
      encryption class, System.Net.NetworkInformation.Ping, and Invoke-Expression for
      potential command execution. These indicators are a sign of PowerDrop malware
      scripts.
      status: experimental
      author: Adlumin
      date: 2023/05/16
      logsource:
        product: windows
        service: powershell
      detection:
        selection1:
          EventID: 4104
          ScriptBlockText: "*RijndaelManaged*"
        selection2:
          EventID: 4104
          ScriptBlockText: "*System.Net.NetworkInformation.Ping*"
        selection3:
          EventID: 4104
          ScriptBlockText: "*Invoke-Expression*"
        condition: selection1 and selection2 and selection3
      level: high
      tags:
        - attack.execution
        - attack.t1059
~~~

Figure 3: SIGMA Rule to detect PowerShell script on endpoint.

Indicators of Compromise

The following IoCs have been identified:

Alias

Needyboy9.2.exe

Hash

MD5

18c78fb8962329ca6115e297c824ecc4

SHA-1

838b3f41c98161c450aa2dec6a3a4b1078195c13

SHA-256

d9477407802b7cb9a4e649055393d99a0d7da8e6b6d6f551aebc4e1849036418

References

https://adlumin.com/post/powerdrop-a-new-insidious-powershell-script-for-command-and-control-attacks-targets-u-s-aerospace-defense-industry/

https://www.bleepingcomputer.com/news/security/new-powerdrop-powershell-malware-targets-us-aerospace-industry/

https://www.dnsfilter.com/blog/c2-server-command-and-control-attack

https://medium.com/@ChahakMittal/powerdrop-the-malware-that-could-disrupt-the-us-aerospace-industry-21049322974b

https://heimdalsecurity.com/blog/new-powerdrop-malware/

https://www.pcrisk.com/removal-guides/27002-powerdrop-malware

VirusTotal - File - d9477407802b7cb9a4e649055393d99a0d7da8e6b6d6f551aebc4e1849036418

https://industrialcyber.co/ransomware/powerdrop-malware-exploits-powershell-script-for-cc-attacks-against-us-aerospace-sector/