# PowerDrop

Threat: **Remote Access Trojan**

Author: **Jeffrey Farnan** Date Originally Published: **June 25th, 2023**

## 1. SUMMARY


- A new malicious PowerShell script called PowerDrop has been found targeting the U.S. aerospace defence industry. It operates as a backdoor or remote access trojan (RAT) by leveraging PowerShell and Windows Management Instrumentation (WMI) to establish a persistent presence within compromised networks. This malware poses significant risks as it grants unauthorized access to compromised systems, allowing cybercriminals to infiltrate networks, steal sensitive data, and execute further malicious actions. It can lead to severe consequences such as data breaches, financial loss, and reputational damage for individuals and organizations.


## 2. MALWARE FAMILY

- **Type** = RAT (Remote Access Trojan).
- **Sub-type** = Spyware.
- **RAT (remote access trojan):** PowerDrop uses PowerShell and WMI (Windows Management Instrumentation) to create a persistent RAT (remote access trojan) on the breached networks.
- **Spyware:** PowerDrop is also a post-exploitation tool, meaning it's designed to gather information from victim networks after obtaining initial access.

## 3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** = May 2023.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = June 20th, 2023.

## 4. MALWARE HISTORY

- PowerDrop was discovered in May 2023 by a company called Adlumin who found a sample of the malware in the network of a defence contractor. The name came from the tool, Windows PowerShell, used to write the script, and 'Drop' from the (DRP) string used in the code. Adlumin has not yet identified the threat actor behind the malware but suspects nation-state aggressors.

## 5. MALWARE DESCRIPTION

- PowerDrop was found in the network of a domestic aerospace defense contractor in May 2023. The malware consists of a novel combination of PowerShell and Windows Management Instrumentation (WMI) as a RAT with persistence. Threat actors typically utilize PowerShell because of its extensive range of features and its capability to avoid detection by leveraging existing infrastructure in commonly used computing environments.
- **Detection:** PowerDrop was detected using machine learning detection that scrutinizes PowerShell script execution content. Exploits, phishing emails, and fraudulent software download sites may have been used by threat actors to distribute PowerDrop.
- **Execution:** The PowerShell script is executed by the Windows Management Instrumentation (WMI) service and encoded using Base64 to function as a backdoor or RAT.
- **Communication:** The malware employs Internet Control Message Protocol (ICMP) echo request messages as beacons to initiate communications with a command-and-control (C2) server. The server, for its part, responds back with an encrypted command that's decoded and run on the compromised host. A similar ICMP ping message is used for exfiltrating the results of the instruction.
- **Information Gathering:** The malware's primary objective is to execute remote commands on targeted networks after successfully infiltrating, executing, and maintaining persistence within servers. PowerDrop enables cybercriminals to exfiltrate valuable information, manipulate compromised systems, install additional malware or backdoors, and execute arbitrary commands, giving them a high level of control over the compromised infrastructure.
- **Evade Detection:** PowerDrop relies on advanced techniques to evade detection, including deception, encoding and encryption.

## 6. POTENTIAL CUSTOMER DEFENSE

- Malicious scripts are unlikely to be detected or blocked by the average anti-malware solution. That’s why cybercriminals are turning to script-based attacks and other evasive malware more often than ever before. As malicious scripts are becoming more widespread, the average user needs to stay protected. Here are some helpful tips:
    - **Exercise caution** - When opening email attachments or clicking on links, especially if they come from unknown or suspicious sources. Do not trust ads and links on suspicious websites. Download software

and files from reputable sources, such as official websites or app stores, and be wary of third-party download sites that may bundle malware with legitimate software.

- **Keep all applications up to date** – Outdated software may contain vulnerabilities criminals are looking to exploit. Check all Windows and third-party apps regularly for updates to lower your risk.
- **Disable macros and script interpreters** – While macros have legitimate applications, most home or business users are unlikely to need them. If a file you or another employee downloaded instructs you to enable macros to view it, don't do it. This is another common evasive tactic that cybercriminals use to get malware onto your system. IT admins should ensure macros and script interpreters are fully disabled to help prevent script-based attacks.
- **Remove unused third-party apps** – Applications such as Python and Java are often unnecessary. If present and unused, simply remove them to help close a number of potential security gaps.
- **Educate end users** – Cybercriminals specifically design attacks to take advantage of end users' trust, naiveté, fear and general lack of technical or security expertise. Educating end users on the risks of cyber-attacks, how to avoid them, and when and how to report them to IT personnel can drastically improve the business' overall security posture and its cyber resilience.
- **Use endpoint security** that provides multiple layers of protections from threats, including file-based, fileless, obfuscated, and encrypted threats.

**Research Sources:**


- https://howtofix.guide/powerdrop-malware/
- https://thehackernews.com/2023/06/new-powerdrop-malware-targeting-us.html
- https://cyware.com/news/new-powerdrop-malware-targets-us-aerospace-industry-146aa0d1
- https://www.secureworld.io/industry-news/powerdrop-cyber-threat-aerospace-industry
- https://unifiedguru.com/powerdrop-powershell-malware-targets-us-aerospace-industry/
- https://www.helpnetsecurity.com/2020/09/07/how-to-protect-yourself-from-the-hidden-threat-of-evasive-scripts/
- https://www.bleepingcomputer.com/news/security/new-powerdrop-powershell-malware-targets-us-aerospace-industry/