POWERSOURCE, Software S0145 | MITRE ATT&CK®

POWERSOURCE is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped. [1] [2]

ⓘ

Associated Software: DNSMessenger

Last Modified: 16 April 2025

Associated Software Descriptions

Name	Description
DNSMessenger	Based on similar descriptions of functionality, it appears S0145, as named by FireEye, is the same as the first stages of a backdoor named DNSMessenger by Cisco's Talos Intelligence Group. However, FireEye appears to break DNSMessenger into two parts: S0145 and S0146. [2] [1]

Techniques Used

Groups That Use This Software

References

1. Miller, S., et al. (2017, March 7). FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings. Retrieved March 8, 2017.
2. Brumaghin, E. and Grady, C.. (2017, March 2). Covert Channels and Poor Decisions: The Tale of DNSMessenger. Retrieved March 8, 2017.