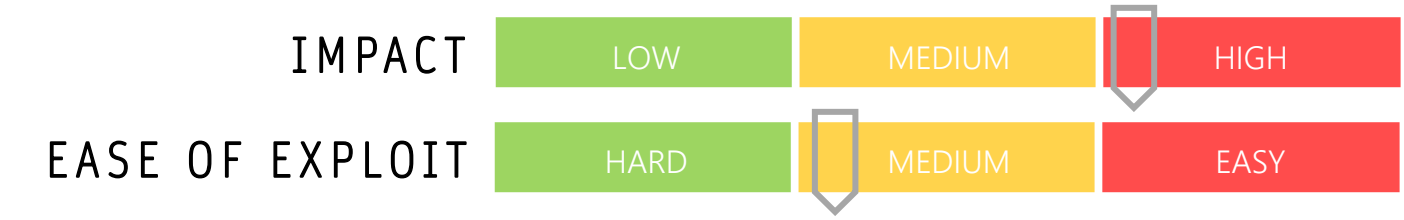
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00071

POWERSHELL BACKDOORS REVEALED IN MS EXCHANGE

DATE ISSUED: 16th November 2020



OVERVIEW

Researchers have discovered two brand new PowerShell backdoors in the Microsoft Exchange Server after an attack on an organization in Kuwait.

BREAKDOWN

Dubbed "TriFive" and "Snugy," these backdoors were used to attack a Kuwait government agency where attackers converted channels for C2 communications – DNS tunnelling and an email-based channel by using the 'Drafts' and 'Deleted Items' folders in compromised email accounts. While little information is currently available as to how the attacker gained access to the Exchange Server, there were suspicious looking commands being executed via the Internet Information Services (IIS) w3wp.exe process. Tasks were scheduled by the attackers to execute before logs were collected to avoid detection in order to execute PowerShell scripts to a previously compromised server. These scripts then ran every 5 and 30 minutes to achieve attack persistence and attempt to open the "slwow64.ps1" and "OfficeIntegrator.ps1" backdoors.

REMEDIATION STEPS

- Use regular network and system monitoring to detect and take actions against any suspicious behaviours
- Use endpoint protection and scanning to detect abnormal user log in activity
- Ensure security patches are applied regularly to keep systems up to date

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/microsoft-exchange-attack-xhunt-backdoors/161041/
Security Affairs: https://securityaffairs.co/wordpress/110644/apt/xhunt-attackers-hit-microsoft-exchange.html
Cyber Security News: https://thecybersecurity.news/vulnerabilities/microsoft-exchange-attack-exposes-new-xhunt-backdoors-3237/