Atacuri cibernetice direcționate cu livrare de malware prin spear-phishing .lnk

Context general	• Ținte: Ministere, agenții guvernamentale și infrastructură critică din Europa de Est. • Actor suspectat: Grupare asociată cu Rusia, posibil APT28 (Fancy Bear) sau afiliat.
Vectorul de atac și metode utilizate	**1. Vector de inițiere** • Emailuri de phishing (spear-phishing), trimise către funcționari guvernamentali. • Atașamente malițioase sub formă de: ➢ Documente ***.docx*** cu macro. ➢ Fișiere ***.lnk*** disimulate ca PDF-uri. ➢ Arhive ***.zip*** cu executabile. **2. Metoda principală de livrare:** • Exploatarea utilizatorului pentru a rula manual fișierul (***User Execution – MITRE T1204***) • Descărcare și execuție payload suplimentar de pe C2 (stage 2 malware)
Payload malware COOKBOX	**Funcționalități observate**: • Acces la fișiere locale și directoare sensibile. • Capturi de ecran periodice. • Monitorizare clipboard (pentru parole/copiere de date). • Persistență în sistem prin Registry sau Task Scheduler. • Exfiltrare de date prin conexiuni HTTPS criptate.
Infrastructura C2	**Domenii și IP-uri implicate:** • ***outlook-updates[.]org*** • ***sec-policy[.]net*** • Adrese IP înregistrate în Rusia și Belarus • Comunicarea se face prin protocoale criptate (HTTPS/443)
IoCs	• Hash malware 3f72bda87312d9b2ee17ab47ff54e6d0 • C2 Domain outlook-updates[.]org • Proces folosit powershell.exe -enc ... • RegKey creat HKCU\Software\Microsoft\Windows\Run\cookbox
Analiză tehnică-Malware COOKBOX	**1. Comportament post-execuție:** • Creează directoare ascunse în %APPDATA% pentru stocarea temporară a fișierelor extrase. • Rulează comenzi sistem prin PowerShell, ex: „ Get-Clipboard Get-ChildItem -Recurse -Path "C:\Users" ” • Deschide conexiuni HTTP/HTTPS criptate la C2 la intervale regulate. **2. Persistență:** • Task Scheduler Task: ***cookbox-updater*** • Script ascuns cu extensie ***.vbs*** în ***%TEMP%:*** „ Set objShell = CreateObject("Wscript.Shell") objShell.Run "powershell -windowstyle hidden -exec bypass ..." ”

Atacuri cibernetice direcționate cu livrare de malware prin spear-phishing .lnk

Instrumente recomadate pentru detecție și analiză	1. **EDR/SIEM**: • SentinelOne, CrowdStrike, Microsoft Defender for Endpoint (pentru semnături comportamentale) • Elastic SIEM sau Splunk pentru căutări IoC: „ index=sysmon sourcetype="powershell" powershell_command="*enc*" ” **2. Sandbox/analiză statică** • Any.run – pentru detonare LNK sau VBS • Intezer Analyze – pentru ADN malware • VirusTotal Intelligence – pentru urmărirea familiilor legate de COOKBOX
Redomandări	✓ Verifică atașamente .lnk în emailuri. ✓ Setați alerte pentru rularea PowerShell cu argumente base64. ✓ Căutați fișiere ***cookbox.exe***, ***agent32.ps1*** în ***%TEMP%***. ✓ Blocați domeniile C2 în DNS și proxy. ✓ Revederea controlului acces pentru conturi de nivel înalt. https://thehackernews.com/2025/04/cert-ua-reports-cyberattacks-targeting.html