APT28 Nearest Neighbor Campaign | MITRE ATT&CK®

Источник: https://attack.mitre.org/campaigns/C0051/
Сохранено в архиве decolonial.ist: 29.08.2026 · файлов в оригинале: 1
Тот же файл в листе: стр. 38 — Campaign C0026 | MITRE ATT&CK®

APT28 Nearest Neighbor Campaign was conducted by APT28 from early February 2022 to November 2024 against organizations and individuals with expertise on Ukraine. APT28 primarily leveraged living-off-the-land techniques, while leveraging the zero-day exploitation of CVE-2022-38028. Notably, APT28 leveraged Wi-Fi networks in close proximity to the intended target to gain initial access to the victim environment. By daisy-chaining multiple compromised organizations nearby the intended target, APT28 discovered dual-homed systems (with both a wired and wireless network connection) to enable Wi-Fi and use compromised credentials to connect to the victim network.[1]

ID	Name	Description
G0007	APT28	APT28 Nearest Neighbor Campaign was conducted by APT28 from early February 2022 to November 2024.[1]

Domain	ID		Name	Use
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	During APT28 Nearest Neighbor Campaign, APT28 used built-in PowerShell capabilities (`Compress-Archive` cmdlet) to compress collected data.[1]
Enterprise	T1110	.003	Brute Force: Password Spraying	During APT28 Nearest Neighbor Campaign, APT28 performed password-spray attacks against public facing services to validate credentials.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During APT28 Nearest Neighbor Campaign, APT28 used PowerShell cmdlet `Get-ChildItem` to access credentials, among other PowerShell functions deployed.[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	During APT28 Nearest Neighbor Campaign, APT28 used `cmd.exe` for execution.[1]
Enterprise	T1584		Compromise Infrastructure	During APT28 Nearest Neighbor Campaign, APT28 compromised third-party infrastructure in physical proximity to targets of interest for follow-on activities.[1]
Enterprise	T1074	.001		

			Data Staged: Local Data Staging	During APT28 Nearest Neighbor Campaign, APT28 staged captured credential information in the `C:\ProgramData` directory.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	During APT28 Nearest Neighbor Campaign, APT28 unarchived data using the GUI version of WinRAR.[1]
Enterprise	T1006		Direct Volume Access	During APT28 Nearest Neighbor Campaign, APT28 accessed volume shadow copies through executing `vssadmin` in order to dump the NTDS.dit file.[1]
Enterprise	T1686	.003	Disable or Modify System Firewall: Windows Host Firewall	During APT28 Nearest Neighbor Campaign, APT28 added rules to a victim's Windows firewall to set up a series of port-forwards allowing traffic to target systems.[1]
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	During APT28 Nearest Neighbor Campaign, APT28 used the native Microsoft utility cipher.exe to securely wipe files and folders – overwriting the deleted data using `cmd.exe /c cipher /W:C` .[1]
Enterprise	T1567		Exfiltration Over Web Service	During APT28 Nearest Neighbor Campaign, APT28 exfiltrated data over public-facing webservers – such as Google Drive.[1]

Enterprise	T1003	.002	OS Credential Dumping: Security Account Manager	During APT28 Nearest Neighbor Campaign, APT28 used the following commands to dump SAM, SYSTEM, and SECURITY hives:
				
				`reg save hklm\sam, reg save hklm\system,`
				
				and
				
				`reg save hklm\security`
				
				.[1]

		.003	OS Credential Dumping: NTDS	During APT28 Nearest Neighbor Campaign, APT28 dumped NTDS.dit through creating volume shadow copies via `vssadmin` .[1]
Enterprise	T1090	.001	Proxy: Internal Proxy	During APT28 Nearest Neighbor Campaign, APT28 used the built-in

				`netsh portproxy` command to create internal proxies on compromised systems.[1]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	During APT28 Nearest Neighbor Campaign, APT28 used RDP for lateral movement.[1]
		.002	Remote Services: SMB/ Windows Admin Shares	During APT28 Nearest Neighbor Campaign, APT28 leveraged SMB to transfer files and move laterally.[1]
Enterprise	T1016	.002	System Network Configuration Discovery: Wi-Fi Discovery	During APT28 Nearest Neighbor Campaign, APT28 collected information on wireless interfaces within range of a compromised system.[1]
Enterprise	T1669		Wi-Fi Networks	During APT28 Nearest Neighbor Campaign, APT28 established wireless connections to secure, enterprise Wi-Fi networks belonging to a target organization for initial access into the environment.[1]

ID	Name	Description
S1205	cipher.exe	APT28 [1]APT28 Nearest Neighbor Campaign [1]
S0108	netsh	APT28[1]APT28 Nearest Neighbor Campaign[1]