Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defence Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Commercial software used to scan target network (e.g. Advanced Port Scanner).	Vulnerabilities in internet-facing systems exploited to gain access to victim networks. [T1190]	Impacket used to execute WMI to achieve command execution on other systems present in environment; also used "proxychains" to redirect network traffic. [T1047] [T1059.003]	Leveraged Windows Service to execute PowerShell and stay persistent; instructions were to disable PowerShell logging, bypass AMSI protection for PowerShell, download, decrypt and execute a backdoor payload from an attacker-controlled server [T1543]	Exploited PrintNightmare to escalate privileges (CVE-2021-1675 and CVE-2021-34527) [T1068]

Also spotted abusing CVE-2022-24521 to escalate privileges. | Attempted to clear the contents of security logs on compromised systems. [T1070.001]

Modified Windows Registry to disable Windows Defender [T1112] [T1562.001]

Used an AMSI bypass to evade detection - the Windows Command Processor was used to invoke PowerShell which then leveraged Invoke-Expression (IEX).

Legitimate processes corrupted via code injection to evade process-based defences. [T1055]

Attempted to thwart reverse engineering and/or dynamic analysis using various sandbox techniques. [T1497]

Attempted to manipulate the features of files dropped in victim environments to make them appear legitimate. [T1036] | Attempted to extract credentials in two ways - by accessing the active directory global catalog file ntds.dit and by utilizing comsvcs.dll (a well-known way to extract LSASS data). [T1003.001]

Also seen using the Invoke-Kerberoast PowerShploit module to perform a Kerberoast attack to obtain credentials from Active Directory Domain Services. [T1558.003] | Used 'sudo' command to obtain credentials associated with a commercial backup solution, likely to gain access to backups present within environment. [T1033]

Used impacket to enumerate the environment and obtain additional information about the Active Directory configuration in place to identify high value targets and maximise sphere of influence. [T1087]

Used the "nltest" command to enumerate the domain trust relationships within the environment. [T1482]

Used a recon tool called Advanced Port Scanner to identify running services and local network infrastructure. [T1046]

Used the attack path reconnaissance tool Bloodhound before deploying ransomware. [T1482] | Leveraged Windows Remote Desktop Connections to pivot to additional systems. [T1021]

Copied and executed PowerShell scripts on remote systems in the environment while moving from system to system. [T1570]

SMB shares used for lateral movement [T1021.002]

Network drives and other shared storage locations used to deliver payloads. [T1080] | Automated the collection of data. [T1119] | Used tools such as SystemBC and proprietary backdoors to communicate with and control compromised systems. [T1219] | Attempted to exfiltrate sensitive information over SMB (TCP/445) directly from a compromised domain controller - likely chosen as a way to bypass egress filtering. [T1048]

PowerShell scripts were used to exfiltrate data to external C2 servers. [T1020]

Tools such as PowerShell and PsExec used to exfiltrate data directly to C2 servers. [T1041]

Cloud storage transfers used to exfiltrate victim data (Mega.nz, Anonfiles.com, File.io, Sendspace) [T1567.002] | Encrypted data on target systems or on a large numbers of systems in a network to interrupt availability to a system and network resources. [T1486]

Ran a script to change passwords of victims' email accounts. [T1531] |
| PowerShell scripts run to collect data and collect browser-related artefacts when interesting hosts identified.

Information about potentially interesting user accounts and remote servers gathered. [T1595] [T1592] | Initial access also obtained through compromised valid accounts. [T1078] | Windows Batch files used to execute PSexec; PSexec then remotely authenticated and executed PowerShell on remote systems within environment. [T1059.001] [T1596.002]

Used malicious files that create component task schedule objects to facilitate recurring execution of their code. [T1053] | Encrypted Windows Operating functions to preserve compromised system functions. [T1543.003]

Employed malicious files that create an undocumented autostart Registry key to maintain persistence after boot/reboot. [T1547.001]

Directly side-loaded their payloads by planting their own DLL then invoking a legitimate application that executes the payload within that DLL [T1574.002] | | | | | | | | | |