

APT3, Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110, Group G0022

Archived: 2026-04-05 16:30:07 UTC

Enterprise [T1087 .001 Account Discovery: Local Account](#)

[APT3](#) has used a tool that can obtain info about local and global group users, power users, and administrators. ^[4]

Enterprise [T1098 .007 Account Manipulation: Additional Local or Domain Groups](#)

[APT3](#) has been known to add created accounts to local admin groups to maintain elevated access. ^[6]

Enterprise [T1560 .001 Archive Collected Data: Archive via Utility](#)

[APT3](#) has used tools to compress data before exfilling it. ^[6]

Enterprise [T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[APT3](#) places scripts in the startup folder for persistence. ^[3]

Enterprise [T1110 .002 Brute Force: Password Cracking](#)

[APT3](#) has been known to brute force password hashes to be able to leverage plain text credentials. ^[7]

Enterprise [T1059 .001 Command and Scripting Interpreter: PowerShell](#)

[APT3](#) has used PowerShell on victim systems to download and run payloads after exploitation. ^[3]

[.003 Command and Scripting Interpreter: Windows Command Shell](#)

An [APT3](#) downloader uses the Windows command `"cmd.exe" /C whoami` . The group also uses a tool to execute commands on remote computers. ^{[3][4]}

Enterprise [T1136 .001 Create Account: Local Account](#)

[APT3](#) has been known to create or enable accounts, such as `support_388945a0` . ^[6]

Enterprise [T1543 .003 Create or Modify System Process: Windows Service](#)

[APT3](#) has a tool that creates a new service for persistence. ^[3]

Enterprise [T1555 .003 Credentials from Password Stores: Credentials from Web Browsers](#)

[APT3](#) has used tools to dump passwords from browsers. ^[4]

Enterprise [T1005 Data from Local System](#)

[APT3](#) will identify Microsoft Office documents on the victim's computer.^[6]

Enterprise [T1074 .001 Data Staged: Local Data Staging](#)

[APT3](#) has been known to stage files for exfiltration in a single location.^[6]

Enterprise [T1546 .008 Event Triggered Execution: Accessibility Features](#)

[APT3](#) replaces the Sticky Keys binary `C:\Windows\System32\sethc.exe` for persistence.^[6]

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[APT3](#) has a tool that exfiltrates data over the C2 channel.^[8]

Enterprise [T1203 Exploitation for Client Execution](#)

[APT3](#) has exploited the Adobe Flash Player vulnerability CVE-2015-3113 and Internet Explorer vulnerability CVE-2014-1776.^{[1][8]}

Enterprise [T1083 File and Directory Discovery](#)

[APT3](#) has a tool that looks for files and directories on the local file system.^{[8][9]}

Enterprise [T1564 .003 Hide Artifacts: Hidden Window](#)

[APT3](#) has been known to use `-WindowStyle Hidden` to conceal [PowerShell](#) windows.^[3]

Enterprise [T1574 .001 Hijack Execution Flow: DLL](#)

[APT3](#) has been known to side load DLLs with a valid version of Chrome with one of their tools.^{[8][10]}

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[APT3](#) has a tool that can delete files.^[8]

Enterprise [T1105 Ingress Tool Transfer](#)

[APT3](#) has a tool that can copy files to remote machines.^[8]

Enterprise [T1056 .001 Input Capture: Keylogging](#)

[APT3](#) has used a keylogging tool that records keystrokes in encrypted files.^[4]

Enterprise [T1036 .010 Masquerading: Masquerade Account Name](#)

[APT3](#) has been known to create or enable accounts, such as `support_388945a0`.^[6]

Enterprise [T1104 Multi-Stage Channels](#)

An [APT3](#) downloader first establishes a SOCKS5 connection to 192.157.198[.]103 using TCP port 1913; once the server response is verified, it then requests a connection to 192.184.60[.]229 on TCP port 81.^[3]

Enterprise [T1095 Non-Application Layer Protocol](#)

An [APT3](#) downloader establishes SOCKS5 connections for its initial C2.^[3]

Enterprise [T1027 Obfuscated Files or Information](#)

[APT3](#) obfuscates files or information to help evade defensive measures.^[4]

[.002 Software Packing](#)

[APT3](#) has been known to pack their tools.^{[7][1]}

[.005 Indicator Removal from Tools](#)

[APT3](#) has been known to remove indicators of compromise from tools.^[7]

Enterprise [T1003 .001 OS Credential Dumping: LSASS Memory](#)

[APT3](#) has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig."^[4]

Enterprise [T1069 Permission Groups Discovery](#)

[APT3](#) has a tool that can enumerate the permissions associated with Windows groups.^[4]

Enterprise [T1566 .002 Phishing: Spearphishing Link](#)

[APT3](#) has sent spearphishing emails containing malicious links.^[1]

Enterprise [T1057 Process Discovery](#)

[APT3](#) has a tool that can list out currently running processes.^{[8][9]}

Enterprise [T1090 .002 Proxy: External Proxy](#)

An [APT3](#) downloader establishes SOCKS5 connections for its initial C2.^[3]

Enterprise [T1021 .001 Remote Services: Remote Desktop Protocol](#)

[APT3](#) enables the Remote Desktop Protocol for persistence.^[6] [APT3](#) has also interacted with compromised systems to browse and copy files through RDP sessions.^[11]

[.002 Remote Services: SMB/Windows Admin Shares](#)

[APT3](#) will copy files over to Windows Admin Shares (like ADMIN\$) as part of lateral movement.^[4]

Enterprise [T1018 Remote System Discovery](#)

[APT3](#) has a tool that can detect the existence of remote systems. ^{[4][8]}

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

An [APT3](#) downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`. ^[3]

Enterprise [T1218 .011 System Binary Proxy Execution: Rundll32](#)

[APT3](#) has a tool that can run DLLs. ^[8]

Enterprise [T1082 System Information Discovery](#)

[APT3](#) has a tool that can obtain information about the local system. ^{[4][9]}

Enterprise [T1016 System Network Configuration Discovery](#)

A keylogging tool used by [APT3](#) gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway. ^{[4][9]}

Enterprise [T1049 System Network Connections Discovery](#)

[APT3](#) has a tool that can enumerate current network connections. ^{[4][8][9]}

Enterprise [T1033 System Owner/User Discovery](#)

An [APT3](#) downloader uses the Windows command `"cmd.exe" /C whoami` to verify that it is running with the elevated privileges of "System." ^[3]

Enterprise [T1552 .001 Unsecured Credentials: Credentials In Files](#)

[APT3](#) has a tool that can locate credentials in files on the file system such as those from Firefox or Chrome. ^[4]

Enterprise [T1204 .001 User Execution: Malicious Link](#)

[APT3](#) has lured victims into clicking malicious links delivered through spearphishing. ^[1]

Enterprise [T1078 .002 Valid Accounts: Domain Accounts](#)

[APT3](#) leverages valid accounts after gaining credentials for use within the victim domain. ^[4]