APT1, Comment Crew, Comment Group, Comment Panda, Group G0006

Archived: 2026-04-02 12:30:34 UTC

Enterprise T1087 .001 Account Discovery: Local Account

APT1 used the commands `net localgroup`, `net user`, and `net group` to find accounts on the system.[1]

Enterprise T1583 .001 Acquire Infrastructure: Domains

APT1 has registered hundreds of domains for use in operations.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

APT1 has used RAR to compress files before moving them outside of the victim network.[1]

Enterprise T1119 Automated Collection

APT1 used a batch script to perform a series of discovery techniques and saves it to a text file.[1]

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

APT1 has used the Windows command shell to execute commands, and batch scripting to automate execution.[1]

Enterprise T1584 .001 Compromise Infrastructure: Domains

APT1 hijacked FQDNs associated with legitimate websites hosted by hop points.[1]

Enterprise T1005 Data from Local System

APT1 has collected files from a local victim.[1]

Enterprise T1114 .001 Email Collection: Local Email Collection

APT1 uses two utilities, GETMAIL and MAPIGET, to steal email. GETMAIL extracts emails from archived Outlook .pst files.[1]

.002 Email Collection: Remote Email Collection

APT1 uses two utilities, GETMAIL and MAPIGET, to steal email. MAPIGET steals email still on Exchange servers that has not yet been archived.[1]

Enterprise T1585 .002 Establish Accounts: Email Accounts

APT1 has created email accounts for later use in social engineering, phishing, and when registering domains.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

The file name AcroRD32.exe, a legitimate process name for Adobe's Acrobat Reader, was used by APT1 as a name for malware.[1][3]

Enterprise T1135 Network Share Discovery

APT1 listed connected network shares.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

APT1 used publicly available malware for privilege escalation.[1]

.002 Obtain Capabilities: Tool

APT1 has used various open-source tools for privilege escalation purposes.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

APT1 has been known to use credential dumping using Mimikatz.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT1 has sent spearphishing emails containing malicious attachments.[1]

.002 Phishing: Spearphishing Link

APT1 has sent spearphishing emails containing hyperlinks to malicious files.[1]

Enterprise T1057 Process Discovery

APT1 gathered a list of running processes on the system using `tasklist /v`.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

The APT1 group is known to have used RDP during operations.[4]

Enterprise T1016 System Network Configuration Discovery

APT1 used the `ipconfig /all` command to gather network configuration information.[1]

Enterprise T1049 System Network Connections Discovery

APT1 used the `net use` command to get a listing on network connections.[1]

Enterprise T1007 System Service Discovery

APT1 used the commands `net start` and `tasklist` to get a listing of the services on the system.[1]

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

The APT1 group is known to have used pass the hash.[1]

Source: https://attack.mitre.org/groups/G0006/