APT39, ITG07, Chafer, Remix Kitten, Group G0087

Archived: 2026-04-05 18:11:01 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

APT39 has used HTTP in communications with C2.[8][3]

.004 Application Layer Protocol: DNS

APT39 has used remote access tools that leverage DNS in communications with C2.[8]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

APT39 has used WinRAR and 7-Zip to compress an archive stolen data.[1]

Enterprise T1197 BITS Jobs

APT39 has used the BITS protocol to exfiltrate stolen data from a compromised host.[3]

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

APT39 has maintained persistence using the startup folder.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

APT39 has modified LNK shortcuts.[1]

Enterprise T1110 Brute Force

APT39 has used Ncrack to reveal credentials.[1]

Enterprise T1115 Clipboard Data

APT39 has used tools capable of stealing contents of the clipboard.[9]

Enterprise T1059 Command and Scripting Interpreter

APT39 has utilized custom scripts to perform internal reconnaissance.[1][3]

.001 PowerShell

APT39 has used PowerShell to execute malicious code.[8][9]

.005 Visual Basic

APT39 has utilized malicious VBS scripts in malware.[3]

.006 Python

APT39 has used a command line utility and a network scanner written in python.[8][3]

.010 AutoHotKey & AutoIT

APT39 has utilized AutoIt malware scripts embedded in Microsoft Office documents or malicious links.[3]

Enterprise T1136 .001 Create Account: Local Account

APT39 has created accounts on multiple compromised hosts to perform actions within the network.[8]

Enterprise T1555 Credentials from Password Stores

APT39 has used the Smartftp Password Decryptor tool to decrypt FTP passwords.[8]

Enterprise T1005 Data from Local System

APT39 has used various tools to steal files from the compromised host.[9][3]

Enterprise T1074 .001 Data Staged: Local Data Staging

APT39 has utilized tools to aggregate data prior to exfiltration.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

APT39 has used malware to decrypt encrypted CAB files.[3]

Enterprise T1546 .010 Event Triggered Execution: AppInit DLLs

APT39 has used malware to set `LoadAppInit_DLLs` in the Registry key `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows` in order to establish persistence.[3]

Enterprise T1041 Exfiltration Over C2 Channel

APT39 has exfiltrated stolen victim data through C2 communications.[3]

Enterprise T1190 Exploit Public-Facing Application

APT39 has used SQL injection for initial compromise.[9]

Enterprise T1083 File and Directory Discovery

APT39 has used tools with the ability to search for files on a compromised host.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

APT39 has used malware to delete files after they are deployed on a compromised host.[3]

Enterprise T1105 Ingress Tool Transfer

APT39 has downloaded tools to compromised hosts.[9][3]

Enterprise T1056 Input Capture

APT39 has utilized tools to capture mouse movements.[3]

.001 Keylogging

APT39 has used tools for capturing keystrokes.[9][3]

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

APT39 has used malware disguised as Mozilla Firefox and a tool named mfevtpse.exe to proxy C2 communications, closely mimicking a legitimate McAfee file mfevtps.exe.[8][3]

Enterprise T1046 Network Service Discovery

APT39 has used CrackMapExec and a custom port scanner known as BLUETORCH for network scanning.[1][8]

Enterprise T1135 Network Share Discovery

APT39 has used the post exploitation tool CrackMapExec to enumerate network shares.[8]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

APT39 has packed tools with UPX, and has repacked a modified version of Mimikatz to thwart anti-virus detection.[1][8]

.013 Obfuscated Files or Information: Encrypted/Encoded File

APT39 has used malware to drop encrypted CAB files.[3]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT39 has modified and used customized versions of publicly-available tools like PLINK and Mimikatz.[8][10]

Enterprise T1003 OS Credential Dumping

APT39 has used different versions of Mimikatz to obtain credentials.[8]

.001 LSASS Memory

APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

APT39 leveraged spearphishing emails with malicious attachments to initially compromise victims.[1][9][3]

.002 Phishing: Spearphishing Link

APT39 leveraged spearphishing emails with malicious links to initially compromise victims.[1][3]

Enterprise T1090 .001 Proxy: Internal Proxy

APT39 used custom tools to create SOCK5 and custom protocol proxies between infected hosts.[1][8]

.002 Proxy: External Proxy

APT39 has used various tools to proxy C2 communications.[8]

Enterprise T1012 Query Registry

APT39 has used various strains of malware to query the Registry.[3]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

APT39 has been seen using RDP for lateral movement and persistence, in some cases employing the rdpwinst tool for mangement of multiple sessions.[1][8]

.002 Remote Services: SMB/Windows Admin Shares

APT39 has used SMB for lateral movement.[9]

.004 Remote Services: SSH

APT39 used secure shell (SSH) to move laterally among their targets.[1]

Enterprise T1018 Remote System Discovery

APT39 has used NBTscan and custom tools to discover remote systems.[1][8][9]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

APT39 has created scheduled tasks for persistence.[1][8][3]

Enterprise T1113 Screen Capture

APT39 has used a screen capture utility to take screenshots on a compromised host.[9][3]

Enterprise T1505 .003 Server Software Component: Web Shell

APT39 has installed ANTAK and ASPXSPY web shells.[1]

Enterprise T1553 .006 Subvert Trust Controls: Code Signing Policy Modification

APT39 has used malware to turn off the `RequireSigned` feature which ensures only signed DLLs can be run on Windows.[3]

Enterprise T1033 System Owner/User Discovery

APT39 used Remexi to collect usernames from the system.[2]

Enterprise T1569 .002 System Services: Service Execution

APT39 has used post-exploitation tools including RemCom and the Non-sucking Service Manager (NSSM) to execute processes.[8][9]

Enterprise T1204 .001 User Execution: Malicious Link

APT39 has sent spearphishing emails in an attempt to lure users to click on a malicious link.[1][3]

.002 User Execution: Malicious File

APT39 has sent spearphishing emails in an attempt to lure users to click on a malicious attachment.[1][8][9][3]

Enterprise T1078 Valid Accounts

APT39 has used stolen credentials to compromise Outlook Web Access (OWA).[1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

APT39 has communicated with C2 through files uploaded to and downloaded from DropBox.[8]
