Threat Group-3390, Earth Smilodon, TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse, Linen Typhoon, Group G0027

Archived: 2026-04-02 11:10:32 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

A Threat Group-3390 tool can use a public UAC bypass method to elevate privileges.[6]

Enterprise T1087 .001 Account Discovery: Local Account

Threat Group-3390 has used `net user` to conduct internal discovery of systems.[2]

Enterprise T1583 .001 Acquire Infrastructure: Domains

Threat Group-3390 has registered domains for C2.[11]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Threat Group-3390 malware has used HTTP for C2.[3]

Enterprise T1560 .002 Archive Collected Data: Archive via Library

Threat Group-3390 has used RAR to compress, encrypt, and password-protect files prior to exfiltration.[2]

Enterprise T1119 Automated Collection

Threat Group-3390 ran a command to compile an archive of file types of interest from the victim user's directories.[2]

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

Threat Group-3390's malware can add a Registry key to `Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[6][11]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Threat Group-3390 has used PowerShell for execution.[2][4]

.003 Command and Scripting Interpreter: Windows Command Shell

Threat Group-3390 has used command-line interfaces for execution.[2][9]

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

Threat Group-3390's malware can create a new service, sometimes naming it after the config information, to gain persistence.[6][11]

Enterprise T1555 .005 Credentials from Password Stores: Password Managers

Threat Group-3390 obtained a KeePass database from a compromised host.[4]

Enterprise T1005 Data from Local System

Threat Group-3390 ran a command to compile an archive of file types of interest from the victim user's directories.[2]

Enterprise T1074 .001 Data Staged: Local Data Staging

Threat Group-3390 has locally staged encrypted archives for later exfiltration efforts.[2]

.002 Data Staged: Remote Data Staging

Threat Group-3390 has moved staged encrypted archives to Internet-facing servers that had previously been compromised with China Chopper prior to exfiltration.[2]

Enterprise T1030 Data Transfer Size Limits

Threat Group-3390 actors have split RAR files for exfiltration into parts.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

During execution, Threat Group-3390 malware deobfuscates and decompresses code that was encoded with Metasploit’s shikata_ga_nai encoder as well as compressed with LZNT1 compression.[3]

Enterprise T1189 Drive-by Compromise

Threat Group-3390 has extensively used strategic web compromises to target victims.[1][3]

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

Threat Group-3390 has exfiltrated stolen data to Dropbox.[4]

Enterprise T1190 Exploit Public-Facing Application

Threat Group-3390 has exploited the Microsoft SharePoint vulnerability CVE-2019-0604 and CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 in Exchange Server.[5]

Enterprise T1203 Exploitation for Client Execution

Threat Group-3390 has exploited CVE-2018-0798 in Equation Editor.[5]

Enterprise T1068 Exploitation for Privilege Escalation

Threat Group-3390 has used CVE-2014-6324 and CVE-2017-0213 to escalate privileges.[2][12]

Enterprise T1210 Exploitation of Remote Services

Threat Group-3390 has exploited MS17-010 to move laterally to other systems on the network.[9]

Enterprise T1133 External Remote Services

Threat Group-3390 actors look for and use VPN profiles during an operation to access the network using external VPN services.[1] Threat Group-3390 has also obtained OWA account credentials during intrusions that it subsequently used to attempt to regain access when evicted from a victim network.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Threat Group-3390 has performed DLL search order hijacking to execute their payload.[6] Threat Group-3390 has also used DLL side-loading, including by using legitimate Kaspersky antivirus variants as well as `rc.exe`, a legitimate Microsoft Resource Compiler.[1][2][3][9][11]

Enterprise T1562 .002 Impair Defenses: Disable Windows Event Logging

Threat Group-3390 has used appcmd.exe to disable logging on a victim server.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Threat Group-3390 has deleted existing logs and exfiltrated file archives from a victim.[2][4]

.005 Indicator Removal: Network Share Connection Removal

Threat Group-3390 has detached network shares after exfiltrating files, likely to evade detection.[2]

Enterprise T1105 Ingress Tool Transfer

Threat Group-3390 has downloaded additional malware and tools, including through the use of `certutil`, onto a compromised host .[1][4]

Enterprise T1056 .001 Input Capture: Keylogging

Threat Group-3390 actors installed a credential logger on Microsoft Exchange servers. Threat Group-3390 also leveraged the reconnaissance framework, ScanBox, to capture keystrokes.[1][7][3]

Enterprise T1112 Modify Registry

A Threat Group-3390 tool has created new Registry keys under `HKEY_CURRENT_USER\Software\Classes\` and `HKLM\SYSTEM\CurrentControlSet\services`.[6][5]

Enterprise T1046 Network Service Discovery

Threat Group-3390 actors use the Hunter tool to conduct network service discovery for vulnerable systems.[1][9]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Threat Group-3390 has packed malware and tools, including using VMProtect.[4][5]

.013 Obfuscated Files or Information: Encrypted/Encoded File

A Threat Group-3390 tool can encrypt payloads using XOR. Threat Group-3390 malware is also obfuscated using Metasploit's shikata_ga_nai encoder.[6][3][9]

.015 Obfuscated Files or Information: Compression

Threat Group-3390 malware is compressed with LZNT1 compression.[6][3][9]

Enterprise T1588 .002 Obtain Capabilities: Tool

Threat Group-3390 has obtained and used tools such as Impacket, pwdump, Mimikatz, gsecdump, NBTscan, and Windows Credential Editor.[9][1]

.003 Obtain Capabilities: Code Signing Certificates

Threat Group-3390 has obtained stolen valid certificates, including from VMProtect and the Chinese instant messaging application Youdu, for their operations.[11]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Threat Group-3390 actors have used a modified version of Mimikatz called Wrapikatz to dump credentials. They have also dumped credentials from domain controllers.[1][2]

.002 OS Credential Dumping: Security Account Manager

Threat Group-3390 actors have used gsecdump to dump credentials. They have also dumped credentials from domain controllers.[1][2]

.004 OS Credential Dumping: LSA Secrets

Threat Group-3390 actors have used gsecdump to dump credentials. They have also dumped credentials from domain controllers.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Threat Group-3390 has used e-mail to deliver malicious attachments to victims.[4]

Enterprise T1055 .012 Process Injection: Process Hollowing

A Threat Group-3390 tool can spawn `svchost.exe` and inject the payload into that process.[6][3]

Enterprise T1012 Query Registry

A Threat Group-3390 tool can read and decrypt stored Registry values.[6]

Enterprise T1021 .006 Remote Services: Windows Remote Management

Threat Group-3390 has used WinRM to enable remote execution.[2]

Enterprise T1018 Remote System Discovery

Threat Group-3390 has used the `net view` command.[6]

Enterprise T1053 .002 Scheduled Task/Job: At

Threat Group-3390 actors use at to schedule tasks to run self-extracting RAR archives, which install HTTPBrowser or PlugX on other victims on a network.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

Threat Group-3390 has used a variety of Web shells.[9]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Threat Group-3390 has hosted malicious payloads on Dropbox.[4]

.002 Stage Capabilities: Upload Tool

Threat Group-3390 has staged tools, including gsecdump and WCE, on previously compromised websites.[1]

.004 Stage Capabilities: Drive-by Target

Threat Group-3390 has embedded malicious code into websites to screen a potential victim's IP address and then exploit their browser if they are of interest.[8]

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

Threat Group-3390 has compromised the Able Desktop installer to gain access to victim's environments.[5]

Enterprise T1016 System Network Configuration Discovery

Threat Group-3390 actors use NBTscan to discover vulnerable systems.[1]

Enterprise T1049 System Network Connections Discovery

Threat Group-3390 has used `net use` and `netstat` to conduct internal discovery of systems. The group has also used `quser.exe` to identify existing RDP sessions on a victim.[2]

Enterprise T1033 System Owner/User Discovery

Threat Group-3390 has used `whoami` to collect system user information.[4]

Enterprise T1199 Trusted Relationship

Threat Group-3390 has compromised third party service providers to gain access to victim's environments.[12]

Enterprise T1204 .002 User Execution: Malicious File

Threat Group-3390 has lured victims into opening malicious files containing malware.[4]

Enterprise T1078 Valid Accounts

Threat Group-3390 actors obtain legitimate credentials using a variety of methods and use them to further lateral movement on victim networks.[1]

Enterprise T1047 Windows Management Instrumentation

A Threat Group-3390 tool can use WMI to execute a binary.[6]
