GROUPS
Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group
CopyKittens
Dark Caracal
Darkhotel
DarkHydrus
Deep Panda
Dragonfly
Dragonfly 2.0
DragonOK
Dust Storm
Elderwood
Equation
FIN10
FIN4
FIN5
FIN6
FIN7
FIN8
Gallmaker
Gamaredon Group
GCMAN
Gorgon Group
Group5
Honeybee
Ke3chang
Kimsuky
Lazarus Group
Leafminer
Leviathan
Lotus Blossom
Machete
Magic Hound
menuPass
Moafee
Molerats
MuddyWater
Naikon
NEODYMIUM
Night Dragon
OilRig
Orangeworm
Patchwork
PittyTiger
PLATINUM
Poseidon Group
PROMETHIUM
Putter Panda
Rancor
RTM
Sandworm Team
Scarlet Mimic
Silence
SilverTerrier
Soft Cell
Sowbug
Stealth Falcon
Stolen Pencil
Strider
Suckfly
TA459
TA505
Taidoor
TEMP.Veles
The White Company
Threat Group-1314
Threat Group-3390
Thrip
Tropic Trooper
Turla
Winnti Group
WIRTE

Threat Group-3390

Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims. [1] The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors. [2] [3]

ID: G0027
Associated Groups: TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse
Version: 1.2
Created: 31 May 2017
Last Modified: 15 October 2019

Associated Group Descriptions

Name	Description
TG-3390	[1] [4] [6]
Emissary Panda	[8] [4] [3] [6][5]
BRONZE UNION	[2] [4]
APT27	[4] [3] [6]
Iron Tiger	[6]
LuckyMouse	[3] [6]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	Threat Group-3390 has used `net user` to conduct internal discovery of systems.[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	T1088	Bypass User Account Control	A Threat Group-3390 tool can use a public UAC bypass method to elevate privileges.[4]
Enterprise	T1059	Command-Line Interface	Threat Group-3390 has used command-line interfaces for execution.[2][5]
Enterprise	T1043	Commonly Used Port	C2 traffic for most Threat Group-3390 tools occurs over Port Numbers 53, 80, and 443.[1]
Enterprise	T1003	Credential Dumping	Threat Group-3390 actors have used gsecdump and a modified version of Mimikatz called Wrapikatz to dump credentials. They have also dumped credentials from domain controllers.[1][2]
Enterprise	T1002	Data Compressed	Threat Group-3390 has used RAR to compress, encrypt, and password-protect files prior to exfiltration.[2]
Enterprise	T1022	Data Encrypted	Threat Group-3390 has used RAR to compress, encrypt, and password-protect files prior to exfiltration.[2]
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	Data Staged	Threat Group-3390 has staged encrypted archives for exfiltration on Internet-facing servers that had previously been compromised with China Chopper.[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	T1089	Disabling Security Tools	Threat Group-3390 has used appcmd.exe to disable logging on a victim server.[2]
Enterprise	T1038	DLL Search Order Hijacking	Threat Group-3390 has performed DLL search order hijacking to execute their payload.[4]
Enterprise	T1073	DLL Side-Loading	Threat Group-3390 has used DLL side-loading, including by using legitimate Kaspersky antivirus variants in which the DLL acts as a stub loader that loads and executes the shell code.[1][2][3][5]
Enterprise	T1189	Drive-by Compromise	Threat Group-3390 has extensively used strategic web compromises to target victims.[1][3]
Enterprise	T1203	Exploitation for Client Execution	Threat Group-3390 has exploited the Microsoft SharePoint vulnerability CVE-2019-0604.[5]
Enterprise	T1068	Exploitation for Privilege Escalation	Threat Group-3390 has used CVE-2014-6324 to escalate privileges.[2]
Enterprise	T1210	Exploitation of Remote Services	Threat Group-3390 has exploited MS17-101 to move laterally to other systems on the network. [5]
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]
Enterprise	T1107	File Deletion	Threat Group-3390 has deleted existing logs and exfiltrated file archives from a victim.[2]
Enterprise	T1056	Input Capture	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][6][3]
Enterprise	T1112	Modify Registry	A Threat Group-3390 tool can create a new Registry key under `HKEY_CURRENT_USER\Software\Classes\`.[4]
Enterprise	T1046	Network Service Scanning	Threat Group-3390 actors use the Hunter tool to conduct network service discovery for vulnerable systems.[1][5]
Enterprise	T1126	Network Share Connection Removal	Threat Group-3390 has detached network shares after exfiltrating files, likely to evade detection.[2]
Enterprise	T1050	New Service	A Threat Group-3390 tool can create a new service, naming it after the config information, to gain persistence.[4]
Enterprise	T1027	Obfuscated Files or Information	A Threat Group-3390 tool can encrypt payloads using XOR. Threat Group-3390 malware is also obfuscated using Metasploit's shikata_ga_nai encoder as well as compressed with LZNT1 compression.[4][3][5]
Enterprise	T1086	PowerShell	Threat Group-3390 has used PowerShell for execution.[2]
Enterprise	T1055	Process Injection	A Threat Group-3390 tool can spawn svchost.exe and inject the payload into that process.[4][3]
Enterprise	T1012	Query Registry	A Threat Group-3390 tool can read and decrypt stored Registry values.[4]
Enterprise	T1108	Redundant Access	Threat Group-3390 has deployed backup web shells and obtained OWA account credentials during intrusions that it subsequently used to attempt to regain access when evicted from a victim network.[2]
Enterprise	T1060	Registry Run Keys / Startup Folder	A Threat Group-3390 tool can add the binary's path to the Registry key `Software\Microsoft\Windows\CurrentVersion\Run` to add persistence.[4]
Enterprise	T1105	Remote File Copy	After re-establishing access to a victim network, Threat Group-3390 actors download tools including gsecdump and WCE that are staged temporarily on websites that were previously compromised but never used.[1]
Enterprise	T1018	Remote System Discovery	Threat Group-3390 has used the `net view` command.[4]
Enterprise	T1053	Scheduled Task	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	T1071	Standard Application Layer Protocol	Threat Group-3390 malware has used HTTP for C2.[3]
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` to conduct internal discovery of systems. The group has also used quser.exe to identify existing RDP sessions on a victim.[2]
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	T1100	Web Shell	Threat Group-3390 has used a variety of Web shells.[5]
Enterprise	T1047	Windows Management Instrumentation	A Threat Group-3390 tool can use WMI to execute a binary.[4]
Enterprise	T1028	Windows Remote Management	Threat Group-3390 has used WinRM to enable remote execution.[2]

Software

ID	Name	References	Techniques
S0073	ASPXSpy	Threat Group-3390 has used a modified version of ASPXSpy called ASPXTool.[1]	Web Shell
S0020	China Chopper	[1] [2] [4] [5]	Brute Force, Command-Line Interface, Data from Local System, File and Directory Discovery, Network Service Scanning, Remote File Copy, Scripting, Software Packing, Standard Application Layer Protocol, Timestomp, Web Shell
S0032	gh0st RAT	[7]	Command-Line Interface, Commonly Used Port, DLL Side-Loading, File Deletion, Indicator Removal on Host, Input Capture, New Service, Process Discovery, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, Screen Capture, Standard Cryptographic Protocol
S0008	gsecdump	[1]	Credential Dumping
S0070	HTTPBrowser	[1] [2] [4]	Command-Line Interface, Commonly Used Port, DLL Search Order Hijacking, DLL Side-Loading, File and Directory Discovery, File Deletion, Input Capture, Masquerading, Obfuscated Files or Information, Registry Run Keys / Startup Folder, Remote File Copy, Standard Application Layer Protocol
S0398	HyperBro	[5] [3] [6]	DLL Side-Loading, Execution through API, File Deletion, Process Injection, Remote File Copy, Screen Capture, Service Execution, Standard Application Layer Protocol, System Service Discovery
S0357	Impacket	[5]	Credential Dumping, Kerberoasting, LLMNR/NBT-NS Poisoning and Relay, Network Sniffing, Service Execution, Windows Management Instrumentation
S0100	ipconfig	[2]	System Network Configuration Discovery
S0002	Mimikatz	Threat Group-3390 has used a modified version of Mimikatz called Wrapikatz.[2][4]	Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection
S0039	Net	[2]	Account Discovery, Create Account, Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery, Remote System Discovery, Service Execution, System Network Connections Discovery, System Service Discovery, System Time Discovery, Windows Admin Shares
S0072	OwaAuth	[1] [2]	Data Encrypted, DLL Side-Loading, File and Directory Discovery, Input Capture, Masquerading, Standard Application Layer Protocol, Timestomp, Web Shell
S0013	PlugX	[1] [2] [4]	Command-Line Interface, Commonly Used Port, Custom Command and Control Protocol, Deobfuscate/Decode Files or Information, DLL Side-Loading, Execution through API, File and Directory Discovery, Input Capture, Masquerading, Modify Existing Service, Modify Registry, Multiband Communication, Network Share Discovery, New Service, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Standard Application Layer Protocol, Standard Non-Application Layer Protocol, System Network Connections Discovery, Trusted Developer Utilities, Virtualization/Sandbox Evasion, Web Service
S0006	pwdump	[5]	Credential Dumping
S0005	Windows Credential Editor	[1]	Credential Dumping
S0412	ZxShell	[7]	Access Token Manipulation, Command-Line Interface, Commonly Used Port, Connection Proxy, Create Account, Disabling Security Tools, Endpoint Denial of Service, File and Directory Discovery, File Deletion, Hooking, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Process Discovery, Process Injection, Query Registry, Remote Desktop Protocol, Remote File Copy, Remote Services, Rundll32, Screen Capture, Standard Application Layer Protocol, System Information Discovery, System Owner/User Discovery, System Service Discovery, Uncommonly Used Port, Video Capture

References

1. Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, August 5). Threat Group-3390 Targets Organizations for Cyberespionage. Retrieved August 18, 2018.
2. Counter Threat Unit Research Team. (2017, June 27). BRONZE UNION Cyberespionage Persists Despite Disclosures. Retrieved July 13, 2017.
3. Legezo, D. (2018, June 13). LuckyMouse hits national data center to organize country-level waterholing campaign. Retrieved August 18, 2018.
4. Pantazopoulos, N., Henry T. (2018, May 18). Emissary Panda – A potential new malicious tool. Retrieved June 25, 2018.
5. Falcone, R. and Lancaster, T.. (2019, May 28). Emissary Panda Attacks Middle East Government Sharepoint Servers. Retrieved July 9, 2019.
6. Khandelwal, S. (2018, June 14). Chinese Hackers Carried Out Country-Level Watering Hole Attack. Retrieved August 18, 2018.
7. Counter Threat Unit Research Team. (2019, February 27). A Peek into BRONZE UNION's Toolbox. Retrieved September 24, 2019.
8. Gallagher, S.. (2015, August 5). Newly discovered Chinese hacking group hacked [illegible] use as "watering holes". Retrieved January 25, 2016.