APT38

attack.mitre.org/groups/G0082

APT38 is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.[1] Active since at least 2014, APT38 has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which APT38 stole $81 million, as well as attacks against Bancomext (2018) and Banco de Chile (2018); some of their attacks have been destructive.[1][2][3][4]

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.

ID: G0082

ⓘ

Associated Groups: NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust Chollima

Version: 2.0

Created: 29 January 2019

Last Modified: 18 January 2022

Version Permalink
Live Version

Domain	ID	Name	Use

Domain	ID	Name	Use	
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT38 used a backdoor, QUICKRIDE, to communicate to the C2 server over HTTP and HTTPS.[2]
Enterprise	T1217	Browser Bookmark Discovery	APT38 has collected browser bookmark information to learn more about compromised hosts, obtain personal information about users, and acquire details about internal network resources.[1]	
Enterprise	T1110	Brute Force	APT38 has used brute force techniques to attempt account access when passwords are unknown or when password hashes are unavailable.[1]	
Enterprise	T1115	Clipboard Data	APT38 used a Trojan called KEYLIME to collect data from the clipboard.[2]	
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT38 has used PowerShell to execute commands and other operational tasks.[1]

Domain	ID	Name	Use	
		.003	Command and Scripting Interpreter: Windows Command Shell	APT38 has used a command-line tunneler, NACHOCHEESE, to give them shell access to a victim’s machine.[2]
		.005	Command and Scripting Interpreter: Visual Basic	APT38 has used VBScript to execute commands and other operational tasks.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	APT38 has installed a new Windows service to establish persistence.[1]
Enterprise	T1485	Data Destruction	APT38 has used a custom secure delete function to make deleted files unrecoverable.[2]	
Enterprise	T1486	Data Encrypted for Impact	APT38 has used Hermes ransomware to encrypt files with AES256.[2]	
Enterprise	T1005	Data from Local System	APT38 has collected data from a compromised host.[1]	
Enterprise	T1565	.001	Data Manipulation: Stored Data Manipulation	APT38 has used DYEPACK to create, delete, and alter records in databases used for SWIFT transactions.[2]
		.002	Data Manipulation: Transmitted Data Manipulation	APT38 has used DYEPACK to manipulate SWIFT messages en route to a printer.[2]

Domain	ID	Name	Use	
		.003	Data Manipulation: Runtime Data Manipulation	APT38 has used DYEPACK.FOX to manipulate PDF data as it is accessed to remove traces of fraudulent SWIFT transactions from the data displayed to the end user.[2]
Enterprise	T1561	.002	Disk Wipe: Disk Structure Wipe	APT38 has used a custom MBR wiper named BOOTWRECK to render systems inoperable.[2]
Enterprise	T1189	Drive-by Compromise	APT38 has conducted watering holes schemes to gain initial access to victims.[2][1]	
Enterprise	T1083	File and Directory Discovery	APT38 have enumerated files and directories, or searched in specific locations within a compromised host.[1]	
Enterprise	T1562	.003	Impair Defenses: Impair Command History Logging	APT38 has prepended a space to all of their terminal commands to operate without leaving traces in the HISTCONTROL environment.[1]
		.004	Impair Defenses: Disable or Modify System Firewall	APT38 have created firewall exemptions on specific ports, including ports 443, 6443, 8443, and 9443.[1]

Domain	ID	Name	Use	
Enterprise	T1070	.001	Indicator Removal on Host: Clear Windows Event Logs	APT38 clears Window Event logs and Sysmon logs from the system.[2]
		.004	Indicator Removal on Host: File Deletion	APT38 has used a utility called CLOSESHAVE that can securely delete a file from the system. They have also removed malware, tools, or other non-native files used during the intrusion to reduce their footprint or as part of the post-intrusion cleanup process.[2][1]
		.006	Indicator Removal on Host: Timestomp	APT38 has modified data timestamps to mimic files that are in the same folder on a compromised host.[1]
Enterprise	T1105	Ingress Tool Transfer	APT38 used a backdoor, NESTEGG, that has the capability to download and upload files to and from a victim's machine.[2]	
Enterprise	T1056	.001	Input Capture: Keylogging	APT38 used a Trojan called KEYLIME to capture keystrokes from the victim's machine.[2]
Enterprise	T1112	Modify Registry	APT38 uses a tool called CLEANTOAD that has the capability to modify Registry keys.[2]	

Domain	ID	Name	Use	
Enterprise	T1106	Native API	APT38 has used the Windows API to execute code within a victim's system.[1]	
Enterprise	T1135	Network Share Discovery	APT38 has enumerated network shares on a compromised host.[1]	
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	APT38 has used several code packing methods such as Themida, Enigma, VMProtect, and Obsidium, to pack their implants.[2]
Enterprise	T1588	.002	Obtain Capabilities: Tool	APT38 has obtained and used open-source tools such as Mimikatz.[8]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT38 has conducted spearphishing campaigns using malicious email attachments.[1]
Enterprise	T1057	Process Discovery	APT38 leveraged Sysmon to understand the processes, services in the organization.[2]	
Enterprise	T1053	.003	Scheduled Task/Job: Cron	APT38 has used cron to create pre-scheduled and periodic background jobs on a Linux system.[1]

Domain	ID	Name	Use	
		.005	Scheduled Task/Job: Scheduled Task	APT38 has used Task Scheduler to run programs at system startup or on a scheduled basis for persistence.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	APT38 has used web shells for persistence or to ensure redundant access.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	APT38 has identified security software, configurations, defensive tools, and sensors installed on a compromised system.[1]
Enterprise	T1218	.001	System Binary Proxy Execution: Compiled HTML File	APT38 has used CHM files to move concealed payloads.[9]
		.011	System Binary Proxy Execution: Rundll32	APT38 has used rundll32.exe to execute binaries, scripts, and Control Panel Item files and to execute code via proxy to avoid triggering security tools.[1]
Enterprise	T1082	System Information Discovery	APT38 has attempted to get detailed information about a compromised host, including the operating system, version, patches, hotfixes, and service packs.[1]	

Domain	ID	Name	Use	
Enterprise	T1049	System Network Connections Discovery	APT38 installed a port monitoring tool, MAPMAKER, to print the active TCP connections on the local system.[2]	
Enterprise	T1033	System Owner/User Discovery	APT38 has identified primary users, currently logged in users, sets of users that commonly use a system, or inactive users.[1]	
Enterprise	T1569	.002	System Services: Service Execution	APT38 has created new services or modified existing ones to run executables, commands, or scripts.[1]
Enterprise	T1529	System Shutdown/Reboot	APT38 has used a custom MBR wiper named BOOTWRECK, which will initiate a system reboot after wiping the victim's MBR.[2]	
Enterprise	T1204	.002	User Execution: Malicious File	APT38 has attempted to lure victims into enabling malicious macros within email attachments.[1]