Pagina 6 - New Malware Campaign Uses Cloudflare Tunnels to Deliver RATs via Phishing Chains

Classificações de Malware:

- trojan (Trojan)
- rat (Backdoor)
- stealth (Rootkit)
- virus (Virus)
- infected (Virus)
- backdoor (Backdoor)
- ransomware (Ransomware)
- infection (Virus)
- adware (Adware)
- ads (Adware)

A new campaign is making use of Cloudflare Tunnel subdomains to host malicious payloads and deliver them via m
alicious attachments embedded in phishing emails.The ongoing campaign has been codenamedSERPENTINE#CLOUDby Sec
uronix.It leverages "the Cloudflare Tunnel infrastructure and Python-based loaders to deliver memory-injected
payloads through a chain of shortcut files and obfuscated scripts," security researcher Tim Pecksaidin a repor
t shared with The Hacker News.The attack starts with sending payment- or invoice-themed phishing emails bearin
g a link to a zipped document that contains a Windows shortcut (LNK) file. These shortcuts are disguised as do
cuments to trick victims into opening them, effectively activating the infection sequence.The elaborate multi-
step process culminates in the execution of a Python-based shellcode loader that executes payloads packed with
the open-source Donut loader entirely in memory.Securonix said the campaign has targeted the United States, U
nited Kingdom, Germany, and other regions across Europe and Asia. The identity of the threat actor(s) behind t
he campaign is presently unknown, although the cybersecurity company pointed out their English fluency.Thethre
at activity clusteris also notable for its shifting initial access methods, pivoting from internet

shortcut (U
RL) files to using LNK shortcut files masquerading as PDF documents. These payloads are then used to retrieve
additional stages over WebDAV via the Cloudflare Tunnel subdomains.It's worth mentioning here that avariation
of this campaignwas previously documented by eSentire and Proofpoint last year, with the attacks paving the wa
y for AsyncRAT, GuLoader, PureLogs Stealer, Remcos RAT, Venom RAT, and XWorm."While the infrastructure and del
ivery mechanics are very similar, there is definitely evidence to suggest that the SERPENTINE#CLOUD campaign c
ould be a continuation of a prior campaign, though with notable differences," Peck told the Hacker News."The d
ifferences in payload complexity and targeting suggest they may be unrelated or represent distinct threat acto
rs converging on a popular tactic that simply works."Some of these differences include the use of extensive co
de obfuscation, additional stages to help it slide under the radar, and the deployment of Python shellcode loa
ders to deliver the main payloads, as opposed to directly serving commodity malware."Given the similarities, i
t's possible that the same threat actors behind it have retooled and modernized their attack chain, or it's po
ssible that this could be an entirely different threat actor who is capitalizing on known attack chains that p
rove effective," Peck added.The abuse of TryCloudflare offers manifold advantages. For starters, malicious act
ors have long made it harder to detect by using legitimate cloud service providers as a front for their operat
ions, including payload delivery and command-and-control (C2) communication.By using a reputable subdomain ("*
.trycloudflare[.]com") for nefarious ends, it makes it exceedingly tough for defenders to distinguish between
harmful and benign activities, thereby allowing it to evade URL or domain-based blocking mechanisms.Furthermor
e, it obviates the need to register domains or rent VPS servers, as well as allows the attackers to host malic
ious content on a local machine and expose them to the public internet with a temporary

"*.trycloudflare[.]com
" subdomain.The initial infection occurs when the LNK files are launched, causing it to download a next-stage
payload, a Windows Script File (WSF), from a remote WebDAV share hosted on a Cloudflare Tunnel subdomain. The
WSF file is subsequently executed using cscript.exe in a manner without arousing the victim's suspicion."This
WSF file functions as a lightweight VBScript-based loader, designed to execute an external batch file from a s
econd Cloudflare domain," Peck said. "The 'kiki.bat' file serves as the main payload delivery script next in t
he series of stagers. Overall, it's designed for stealth and persistence."The primary responsibility of the ba
tch script is to display a decoy PDF document, check for antivirus software, and download and execute Python p
ayloads, which are then used to run Donut-packed payloads like AsyncRAT or Revenge RAT in memory.Securonix sai
d there is a possibility that the script may have been vibe-coded using a large language model owing to the pr
esence of well-defined comments in the source code."The SERPENTINE#CLOUD campaign is a complex and layered inf
ection chain that blends a bit of social engineering, living-off-the-land techniques, and evasive in-memory co
de execution," the company concluded. "The abuse of Cloudflare Tunnel infrastructure further complicates netwo
rk visibility by giving the actor a disposable and encrypted transport layer for staging malicious files witho
ut maintaining traditional infrastructure."The disclosure comes as Acronis identified an active malware campai
gn dubbedShadow Vectortargeting users in Colombia using booby-trapped scalable vector graphics (SVG) files as
the malware delivery vector in phishing emails that impersonate court notifications."Attackers distributed spe
ar-phishing emails impersonating trusted institutions in Colombia, delivering SVG decoys with embedded links t
o JS / VBS stagers hosted on public platforms, or password-protected ZIP files containing the payloads directl
y," Acronis researchers Santiago Pontiroli, Jozsef Gegeny, and Ilia Dafchevsaid.The attacks

led to the deploym
ent of remote access trojans likeAsyncRATandRemcos RAT, with recent campaigns also utilizing a .NET loader ass
ociated withKatz Stealer. These attack chains involve hiding the payloads within Base64-encoded text of image
files hosted on the Internet Archive.A noteworthy aspect of the campaign is the use ofSVG smugglingtechniques
to deliver malicious ZIP archives using SVG files. These payloads are hosted on file-sharing services such as
Bitbucket, Dropbox, Discord, and YDRAY. The download archives contain both legitimate executables and maliciou
s DLLs, the latter of which are sideloaded to ultimately serve the trojans."A natural evolution from its earli
er SVG smuggling techniques, this threat actor has adopted a modular, memory-resident loader that can execute
payloads dynamically and entirely in memory, leaving minimal traces behind," the researchers said."The presenc
e of Portuguese-language strings and method parameters within the loader mirrors TTPs commonly observed in Bra
zilian banking malware, suggesting potential code reuse, shared development resources or even cross-regional a
ctor collaboration."The findings also coincide with a rise in social engineering attacks that employ theClickF
ixtactic to deploy stealers and remote access trojans like Lumma Stealer and SectopRAT under the guise of fixi
ng an issue or completing a CAPTCHA verification.According to statistics shared by ReliaQuest, drive-by compro
mises accounted for 23% of all phishing-based tactics observed between March and May 2025. "Techniques like Cl
ickFix were central to drive-by downloads," the cybersecurity companysaid.ClickFix is effective primarily beca
use it deceives targets into carrying out seemingly harmless, everyday actions that are unlikely to raise any
red flags, because they're so used to seeing CAPTCHA screening pages and other notifications. What makes it co
mpelling is that it gets users to do the main work of infecting their own machines instead of having to resort
to more sophisticated methods like exploiting software flaws."External remote resources

dropped from third to
fourth place as attackers increasingly exploit user mistakes rather than technical vulnerabilities," ReliaQue
st said. "This shift is likely driven by the simplicity, success rate, and universal applicability of social e
ngineering campaigns like ClickFix."Discover real-time defense tactics to detect and block deepfakes, fake dom
ains, and multi-channel scams before they cause damage.We'll unpack how leading teams are using AI, privacy-fi
rst design, and seamless logins to earn user trust and stay ahead in 2025.Get the latest news, expert insights
, exclusive resources, and strategies from industry leaders all for free.

Link: https://thehackernews.com/2025/02/belarus-linked-ghostwriter-uses.html