Pagina 2 - Google Chrome Zero-Day CVE-2025-2783 Exploited by TaxOff to Deploy Trinper Backdoor

Classificações de Malware:

- cve (Exploit)
- backdoor (Backdoor)
- exploit (Exploit)
- rootkit (Rootkit)
- trojan (Trojan)
- dropper (Trojan)
- rat (Backdoor)
- virus (Virus)

A now-patched security flaw in Google Chrome was exploited as a zero-day by a threat actor known as TaxOff to
deploy a backdoor codenamedTrinper.The attack, observed in mid-March 2025 by Positive Technologies, involved t
he use of a sandbox escape vulnerability tracked as CVE-2025-2783 (CVSS score: 8.3).Googleaddressedthe flaw la
ter that month after Kaspersky reported in-the-wild exploitation in a campaign dubbed Operation ForumTroll tar
geting various Russian organizations."The initial attack vector was a phishing email containing a malicious li
nk," security researchers Stanislav Pyzhov and Vladislav Luninsaid. "When the victim clicked the link, it trig
gered a one-click exploit (CVE-2025-2783), leading to the installation of the Trinper backdoor employed by Tax
Off."The phishing email is said to have been disguised as an invitation to the Primakov Readings forum the sam
e lure detailed by Kaspersky urging users to click on a link that led to a fake website hosting the exploit.Ta
xOff is the name assigned to ahacking groupthat was first documented by the Russian cybersecurity company in l
ate November 2024 as targeting domestic government agencies using legal and finance-related phishing emails to
deliver Trinper.Written in C++, the backdoor makes use of multithreading to capture victim host information,
record keystrokes, gather files matching specific extensions (.doc, .xls, .ppt, .rtf, and .pdf),

and establish
a connection with a remote server to receive commands and exfiltrate the results of the execution.The instruc
tions sent from the command-and-control (C2) server extend the implant's functionality, allowing it to read/wr
ite files, run commands using cmd.exe, launch a reverse shell, change directory, and shutdown itself."Multithr
eading provides a high degree of parallelism to hide the backdoor while retaining the ability to collect and e
xfiltrate data, install additional modules, and maintain communications with C2," Lunin noted at the time.Posi
tive Technologies said its investigation into the mid-March 2025 intrusion led to the discovery of another att
ack dating back to October 2024 that also commenced with a phishing email, which purported to be an invitation
to an international conference called "Security of the Union State in the modern world."That email contained
a link, which downloaded a ZIP archive file containing a Windows shortcut that, in turn, launched a PowerShell
command to ultimately serve a decoy document while also dropping a loader responsible for launching the Trinp
er backdoor by means of the open-sourceDonutloader. A variation of the attack has been found to swap out the D
onut loader in favor of Cobalt Strike.This attack chain, per the company, shares several tactical similarities
with that of another hacking group tracked asTeam46, raising the possibility that the two threat activity clu
sters are one and the same.Interestingly, another set of phishing emails sent by the Team46 attackers a month
before claimed to be from Moscow-based telecom operator Rostelecom, alerting recipients of supposed maintenanc
e outages last year.These emails included a ZIP archive, which embedded a shortcut that launched a PowerShell
command to deploy a loader that had been previously used to deliver another backdoor in an attack targeting an
unnamed Russian company in the rail freight industry.The March 2024 intrusion,detailedby Doctor Web, is notab
le for the fact that one of the payloads weaponized a DLL hijacking vulnerability in Yandex

Browser for Window
s (CVE-2024-6473, CVSS score: 8.4) as a zero-day to download and execute unspecified malware. It wasresolvedin
version 24.7.1.380 released in September 2024."This group leverages zero-day exploits, which enables it to pe
netrate secure infrastructures more effectively," the researchers said. "The group also creates and uses sophi
sticated malware, implying that it has a long-term strategy and intends to maintain persistence on the comprom
ised systems for an extended period."Discover real-time defense tactics to detect and block deepfakes, fake do
mains, and multi-channel scams before they cause damage.We'll unpack how leading teams are using AI, privacy-f
irst design, and seamless logins to earn user trust and stay ahead in 2025.Get the latest news, expert insight
s, exclusive resources, and strategies from industry leaders all for free.

Link: https://amp.thehackernews.com/stories/cybersecurity-06052025.html