'Purple Fox' Hackers Spotted Using New Variant of FatalRAT in Recent Malware Attacks

thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html

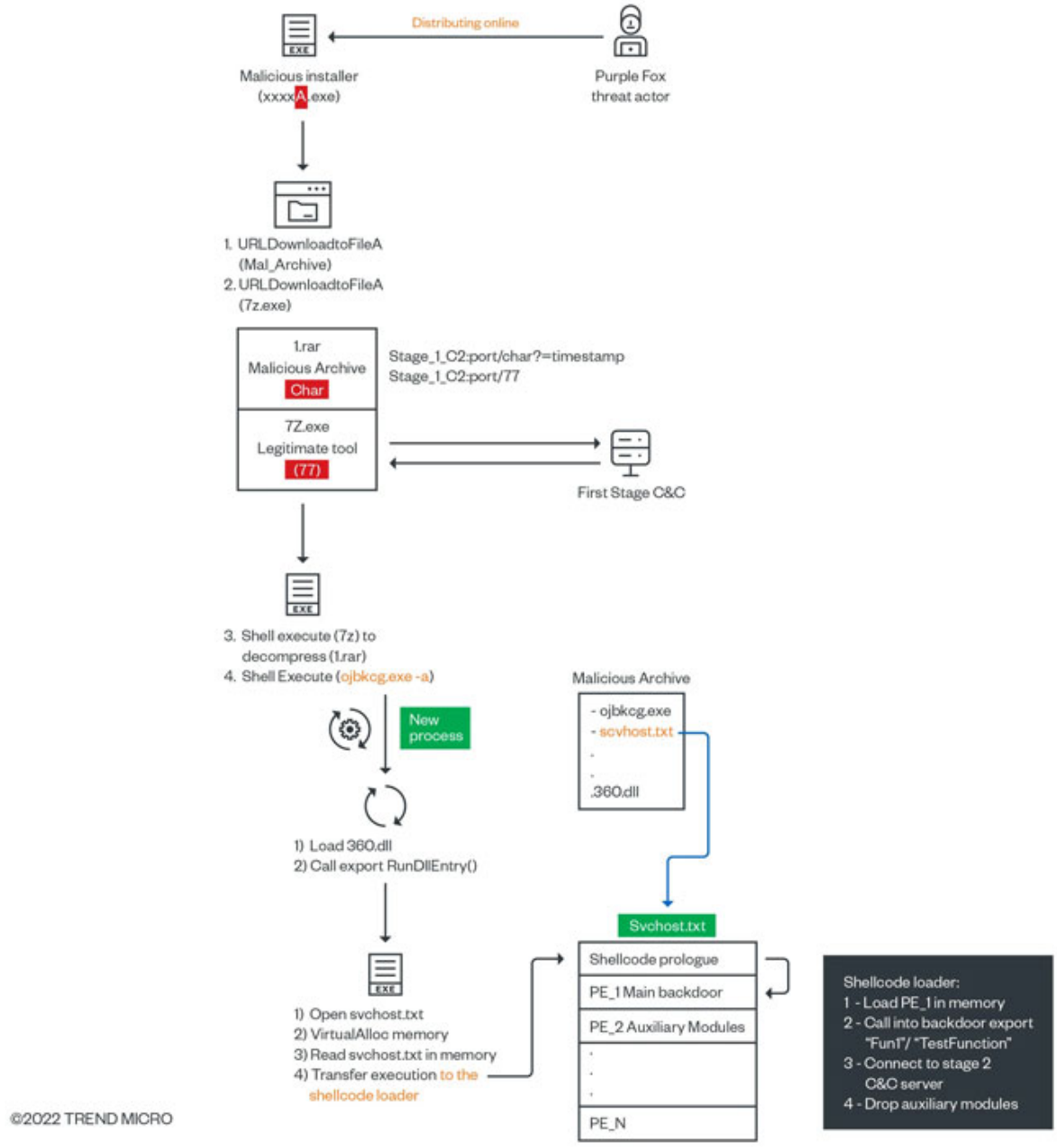
March 28, 2022

The operators of the Purple Fox malware have retooled their malware arsenal with a new variant of a remote access trojan called FatalRAT, while also simultaneously upgrading their evasion mechanisms to bypass security software.

"Users' machines are targeted via trojanized software packages masquerading as legitimate application installers," Trend Micro researchers said in a report published on March 25, 2022. "The installers are actively distributed online to trick users and increase the overall botnet infrastructure."

The findings follow prior research from Minerva Labs that shed light on a similar modus operandi of leveraging fraudulent Telegram applications to distribute the backdoor. Other disguised software installers include WhatsApp, Adobe Flash Player, and Google Chrome.

These packages act as a first-stage loader, triggering an infection sequence that leads to the deployment of a second-stage payload from a remote server and culminating in the execution of a binary that inherits its features from FatalRAT.

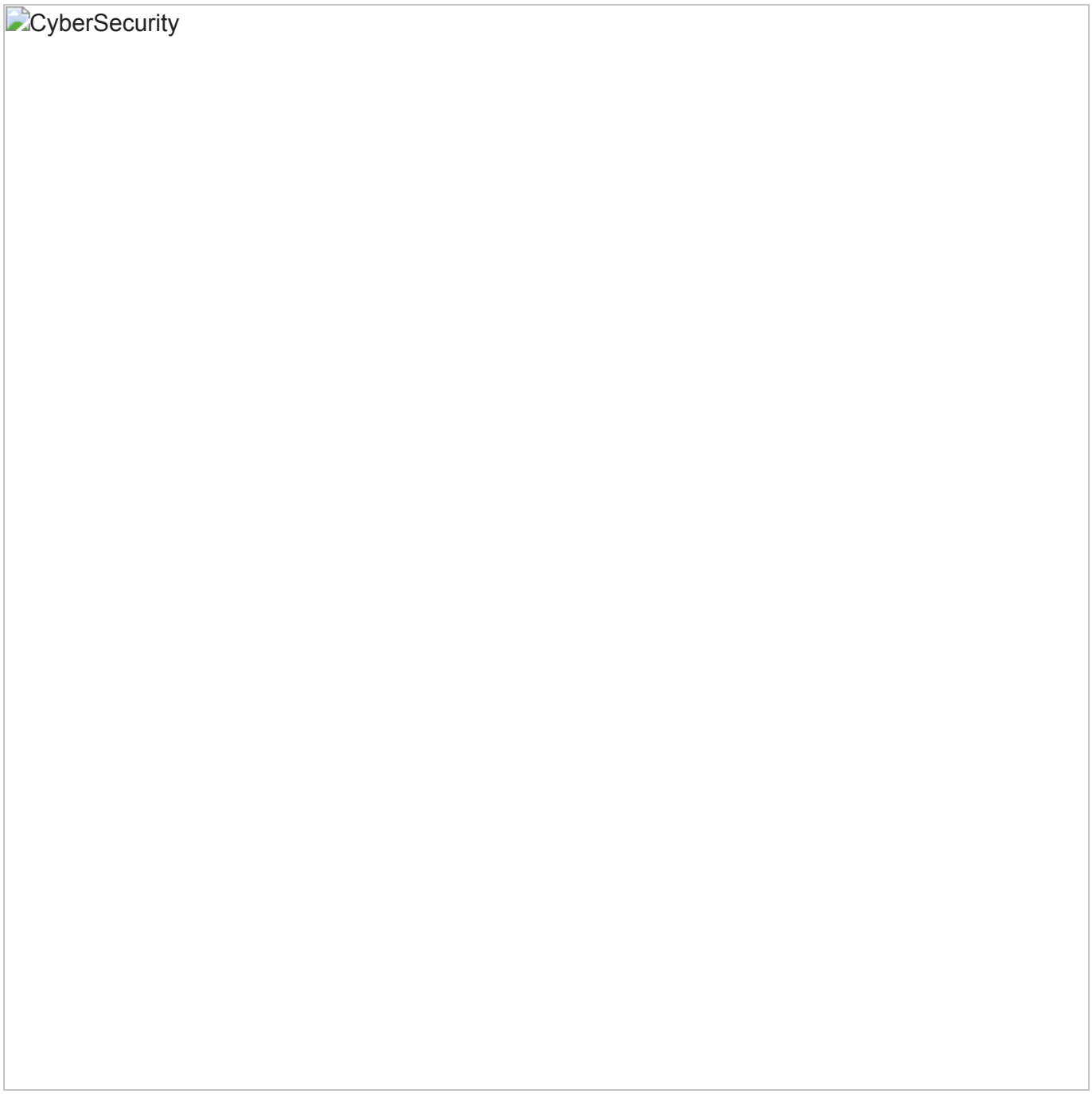


FatalRAT is a C++-based implant designed to run commands and exfiltrate sensitive information back to a remote server, with the malware authors incrementally updating the backdoor with new functionality.

"The RAT is responsible for loading and executing the auxiliary modules based on checks performed on the victim systems," the researchers said. "Changes can happen if specific [antivirus] agents are running or if registry keys are found. The auxiliary modules are intended as support for the group's specific objectives."

Package Description	Weaponized Filename	Distribution Date
Telegram Installer	TextInputh.exe	2021-12-08
360BDoctor software	客户账单明细j.exe	2021-10-17
PPHelper Tool for Windows to Jailbreak iDevices	pphelper5.exe	2021-12-01
Vmware KVM	极品新茶上线到付服务项目以及联系方式r.exe	2021-09-13
ScreenRecorderPro	Apowersoft.ScreenRecorderPro3.exe	2022-01-02
Network Scanner	zenmap.exe	2022-01-18
chrome_pwa_launcher	x.exe	2022-01-22
Whatsapp installer	whatsappsetupr.exe	2022-01-28
Proxifier Proxy Client	(奇迹娱乐12月总账单z.exe)	2022-01-06
Adobe flash installer	flashc.exe	2022-02-07
Micro Focus Net Express	mfcss.exe	2022-02-19
QuickQ Installer	QuickQr.exe	2022-02-21

Furthermore, Purple Fox, which comes with a rootkit module, comes with support for five different commands, including copying and deleting files from the kernel as well as evading antivirus engines by intercepting calls sent to the file system.



The findings also follow recent disclosures from cybersecurity firm Avast, which detailed a new campaign that involved the Purple Fox exploitation framework acting as a deployment channel for another botnet called DirtyMoe.

"Operators of the Purple Fox botnet are still active and consistently updating their arsenal with new malware, while also upgrading the malware variants they have," the researchers said. "They are also trying to improve their signed rootkit arsenal for [antivirus] evasion and trying to bypass detection mechanisms by targeting them with customized signed kernel drivers."

SHARE □ □ □ □ ډ
SHARE □