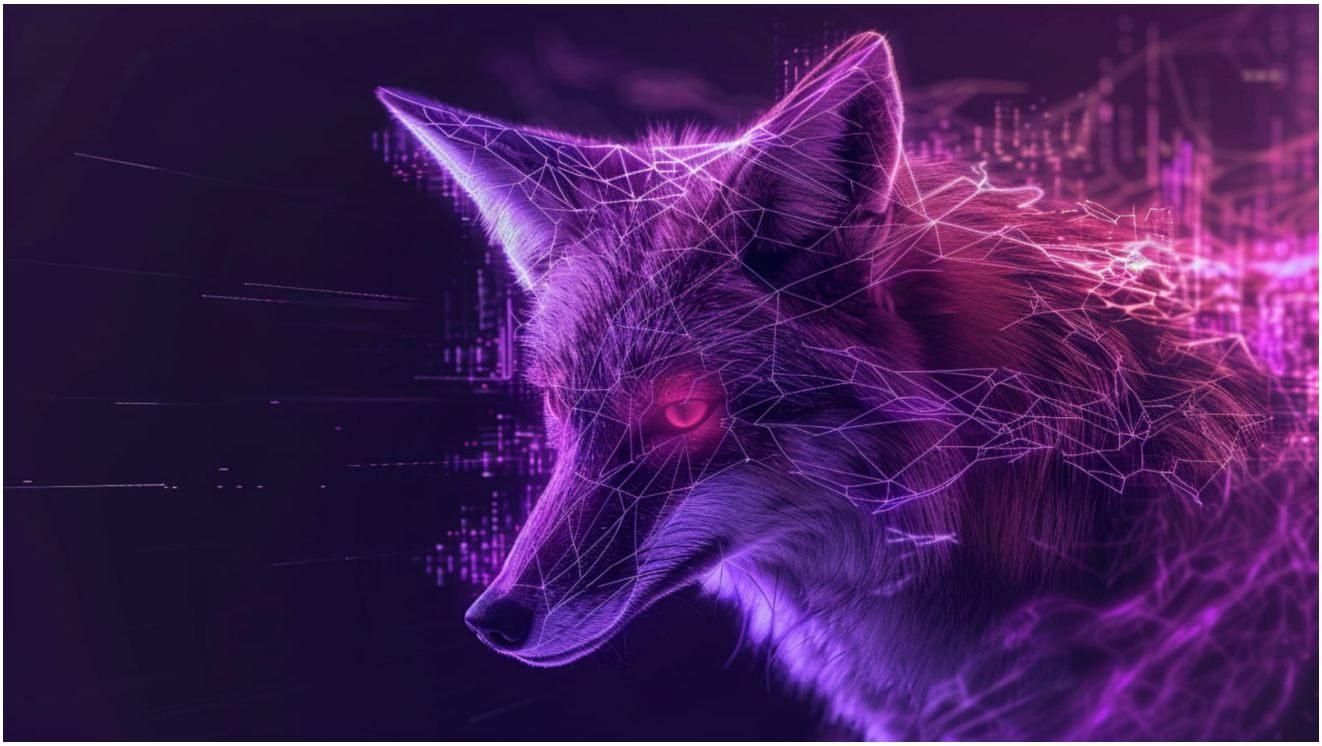
PurpleFox malware infects thousands of computers in Ukraine

bleepingcomputer.com/news/security/purplefox-malware-infects-thousands-of-computers-in-ukraine/

Bill Toulas

By
Bill Toulas

- February 1, 2024
- 12:10 PM
- 0



The Computer Emergency Response Team in Ukraine (CERT-UA) is warning about a PurpleFox malware campaign that has infected at least 2,000 computers in the country.

The exact impact of this widespread infection and whether it has affected state organizations or regular people's computers hasn't been determined, but the agency has shared detailed information on how to locate infections and remove the malware.

PurpleFox (or 'DirtyMoe') is a modular Windows botnet malware first spotted in 2018 that comes with a rootkit module allowing it to hide and persist between device reboots.

It can be used as a downloader that introduces more potent second-stage payloads on compromised systems, offers its operators backdoor capabilities, and can also act as a distributed denial of service (DDoS) bot.

In October 2021, researchers noticed that new versions of PurpleFox switched to using WebSocket for command and control (C2) communications for stealth. In January 2022, a campaign spread the malware under the guise of a Telegram desktop app.

Ukrainian infection wave

CERT-UA used IoCs shared by Avast and TrendMicro to identify PurpleFox malware infections on Ukrainian computers, tracking the activity under the identifier 'UAC-0027.'

"In the process of a detailed study of the cyber threat, research was conducted on the samples of malicious software received, the characteristics of the operating infrastructure of the control servers were identified, and more than 2000 infected computers in the Ukrainian segment of the internet were discovered," explains CERT-UA in a machine-translated security warning.

CERT-UA says PurpleFox typically infects systems when victims launch laced MSI installers and highlights its self-propagation capabilities using exploits for known flaws and password brute-forcing.

The agency recommends isolating systems that run outdated OS versions and software using VLAN or physical network segmentation with incoming/outgoing filtering to prevent spreading.

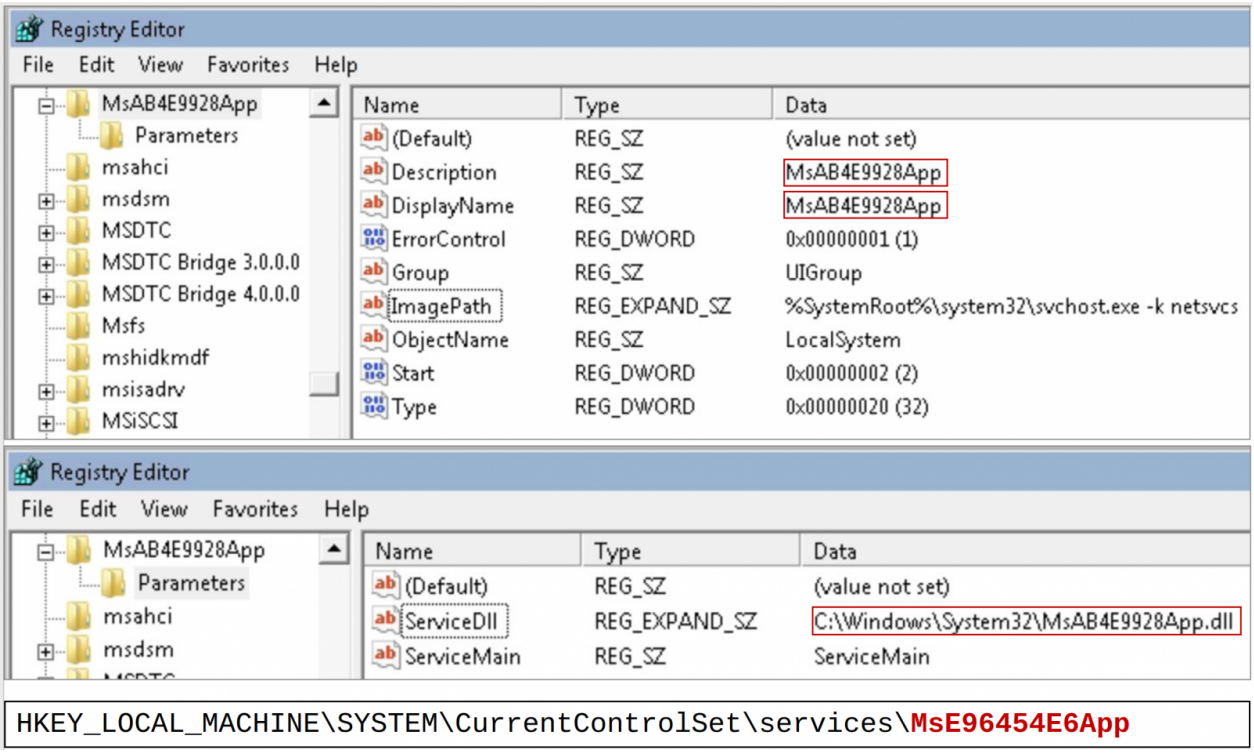
CERT-UA monitored infected hosts between January 20 and 31, 2024, detecting 486 intermediate control server IP addresses, most of which are located in China.

CERT-UA notes that PurpleFox's removal is challenging due to its use of a rootkit, but there are still effective methods that can help detect and uproot the malware.

First, to discover PurpleFox infections, users are recommended to do the following:

1. Examine network connections to "high" (10000+) ports using the IP address list in the report's appendix.
2. Use regedit.exe to check for the following registry values:
3. WindowsXP: HKEY_LOCAL_MACHINE\ControlSet001\Services\AC0[0-9]
4. Windows7: HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlay8\Direct3D
5. Analyze "Application" log in Event Viewer for event IDs 1040 and 1042, source: "MsiInstaller"
6. Check "C:\Program Files" for folders with random names, e.g., "C:\Program Files\dvhvA"
7. Verify the persistent execution of the malware, which uses services and stores files in specific directories, impeded by a rootkit from detection/removal. Key locations are:
8. HKEY_LOCAL_MACHINE\System\ControlSet001\services\MsXXXXXXXXApp
9. C:\Windows\System32\MsXXXXXXXXApp.dll

10. C:\Windows\AppPatch\DBXXXXXXXXMK.sdb, RCXXXXXXXXMS.sdb, TKXXXXXXXXMS.sdb
11. (where XXXXXXXX is a random [A-F0-9]{8} sequence, e.g., "MsBA4B6B3AApp.dll")



Services added for persistence *(CERT-UA)*

If any of the above indicates PurpleFox infection, CERT-UA suggests either using Avast Free AV to run a "SMART" scan and remote all modules or perform the following steps:

1. Boot from LiveUSB or connect the infected drive to another computer
2. Manually delete "MsXXXXXXXXApp.dll" and ".sdb" modules
3. Boot normally and remove the service from the registry

For disk operations:

- Use lsblk and fdisk -lu /dev/sda to identify partitions
- Mount the system partition in read-write mode: mount -orw,offset=$((512*206848)) /dev/sda /mnt/
- Search and remove files in /mnt/Windows/AppPatch and /mnt/Windows/System32 (e.g., ls -lat /mnt/Windows/AppPatch/ and rm -rf /mnt/Windows/AppPatch/RC2EE39E00MS.sdb)
- Unmount with umount /mnt/

After cleaning, to avoid re-infection from PurpleFox, which is very likely if there are still infected machines on the same network, enable the firewall on Windows and create a rule to block incoming traffic from ports 135, 137, 139, and 445.

Related Articles:

No, 3 million electric toothbrushes were not used in a DDoS attack

Bigpanzi botnet infects 170,000 Android TV boxes with malware

Hacker arrested for selling bank accounts of US, Canadian users

Zeus, IcedID malware gangs leader pleads guilty, faces 40 years in prison

FBI: Androxgh0st malware botnet steals AWS, Microsoft credentials