Mphasis
The Next Applied

PlugX Malware

Date: 28th April 2024 | Severity: High

Summary

As malicious actors across the threat landscape continue to pursue more efficient and effective ways of compromising target networks, all while remaining undetected by security measures, it is unsurprising to see an increase in the use of remote access trojans (RATs) in recent years. RATs typically operate stealthily, evading security tools while offering threat actors remote control over infected devices, allowing attackers to execute a wide range of malicious activities like data theft or installing additional malware.

Attack Vectors

The worm adds to the connected flash drive a Windows shortcut file with the drive's name, and three files for DLL sideloading, namely a legitimate executable, a malicious library, and a binary blob within the drive's RECYCLER.BIN hidden folder. It also moves the drive's contents to a new directory. Then the user clicks on the shortcut file, the malware opens a new window displaying the drive's contents, and then copies itself to the system and creates a new registry key for persistence. Next, it re-executes itself from the system, where it checks every 30 seconds for connected USB drives to infect.

Indicator of compromise

INDICATOR TYPE	INDICATORS
IOCs	• 45.142.166[.]112 - IP - PlugX C2 Endpoint / moderate – high • 103.56.53[.]46 - IP - PlugX C2 Endpoint / moderate – high • Mozilla/5.0 (Windows NT 10.0;Win64;x64)AppleWebKit/537.36 - User Agent - PlugX User Agent / moderate – high • /8891431c - URI - PlugX URI / moderate-high • /ba12b866 - URI - PlugX URI / moderate –high
File Hash	• 432a07eb49473fa8c71d50ccaf2bc980b692d458ec4aaedd52d739cb377f3428 • e8f55d0f327fd1d5f26428b890ef7fe878e135d494acda24ef01c695a2e9136d • 3a53bd36b24bc40bdce289d26f1b6965c0a5e71f26b05d19c7aa73d9e3cfa6ff • 2304891f176a92c62f43d9fd30cae943f1521394dce792c6de0e097d10103d45 • 8b8adc6c14ed3bbeacd9f39c4d1380835eaf090090f6f826341a018d6b2ad450 • 6bb959c33fdfc0086ac48586a73273a0a1331f1c4f0053ef021eebe7f377a292 • B9f3cf9d63d2e3ce1821f2e3eb5acd6e374ea801f9c212eebfa734bd649bec7a

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security softwares with the latest available and validated patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://darktrace.com/blog/plugx-malware-a-rats-race-to-adapt-and-survive
- https://blog.sekoia.io/unplugging-plugx-sinkholing-the-plugx-usb-worm-botnet/