Published on *The National Law Review* https://natlawreview.com

Ankura CTIX FLASH Update - January 6, 2023

Article By:

Ankura Cyber Threat Investigations and Expert Services

Malware Activity

New Phishing Campaign Utilizes Fraudulent Shops "Selling" Flipper Zero Products

Security-interested members of the Flipper Zero community are being targeted by a new phishing campaign. Flipper Zero is a portable Tamagotchi-like multi-functional cybersecurity tool used to interact with access control systems. Since its Kickstarter campaign was launched in 2020, security researchers have demonstrated the product's capabilities on social media, which generated interest in the infosec community for the release of the product. Threat actors have begun to take advantage of this interest and lack of product availability in 2022 by creating fraudulent Twitter accounts and shops that claim to be selling the product. One (1) of the two (2) currently identified shops is still online as of January 4, 2022, and is claiming to sell the Flipper Zero, the Wi-Fi module, and the case at the same price as the products on the legitimate website. The phishing campaign's apparent goal is to obtain the victims' email addresses, full names, and shipping addresses. The buyers are able to "pay" for the products with Ethereum or Bitcoin cryptocurrency. It is noted that the shop may use new wallets after each transaction, as the wallet on the site as of January 4 has not received any payments. As interest about Flipper Zero remains and the shortage of product continues, it is expected that actors will continue to target the community. CTIX analysts will continue to monitor for newly discovered phishing campaigns and provide context regarding notable incidents.

- Bleeping Computer: Flipper Zero Article
- Bitdefender: Flipper Zero Article

Threat Actor Activity

Threat Profile: Blind Eagle/APT-C-36

Threat actors associated with the Blind Eagle threat organization (APT-C-36) have recently launched major phishing operations in an apparent resurgence of the group. Active since 2018, Blind Eagle is a financially motivated organization targeting entities throughout various South American countries, including entities within manufacturing, financial, and oil/gas industries. This type of activity has been seen in the apparent resurgence from the group during their recent campaign. Blind Eagle actors launched campaigns with improved infection chains and customized tooling, mainly targeting organizations in Colombia and Ecuador. Phishing emails distributed by threat actors in this campaign generically imitate a government institution and contain a malicious URL and PDF file attachment. Unlike other recent phishing campaigns, Blind Eagle threat actors employ a geofencing protocol to only execute malicious code for users within the allowed area (in this case, Colombia, and Ecuador). Otherwise, the malicious code will not execute and the user will be redirected to a legitimate website of the imitated government entity. The malware, "QuasarRAT", detonated in this campaign is unusual in the fact that the malware is typically associated with cyber-espionage operations from other threat organizations. Analysis of the embedded code shows that Blind Eagle actors utilized QuasarRAT to gather banking information from these compromised devices, fitting their modus operandi. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

- Checkpoint: Blind Eagle Article

Vulnerabilities

Synology Patches Multiple Critical Vulnerabilities

In a published advisory, networking device manufacturer Synology stated that it patched a critical remote code execution (RCE) vulnerability affecting their VPN Plus Server solution for Synology Router Manager (SRM). The flaw, tracked as CVE-2022-43931, received the maximum severity with a CVSS score of 10/10. The vulnerability is described as an out-of-bounds write flaw specifically impacting the remote desktop functionality and could be exploited by threat actors to remotely execute arbitrary code and commands on the target system. VPN Plus is an add-on package that enables Synology NAS devices to become VPN servers, allowing Synology DiskStation Manager (DSM) users over the internet to securely access the resources shared in a Synology device's network. Successful exploitation of this vulnerability could allow threat actors to completely take over a vulnerable system and carry out devastating follow-on attacks. A week prior to Synology's RCE advisory, the company released a patch advisory for multiple other vulnerabilities (some were demonstrated at the December 2022 Pwn2Own contest) which could allow remote attackers to execute arbitrary commands, conduct denial-of-service (DoS) attacks or read arbitrary files after exploiting a vulnerable version of SRM. These are very low-complexity attacks which could be exploited by unsophisticated threat actors. To prevent exploitation of any of the vulnerabilities, CTIX analysts urge all SRM users to immediately update to the latest secure version of their device firmware. Specific details surrounding the updates can be found in the Synology advisories linked below.

- The Hacker News: CVE-2022-43931 Article
- Synology: CVE-2022-43931 Advisory
- Synology: Multiple Vulnerabilities Advisory

Source URL:https://natlawreview.com/article/ankura-ctix-flash-update-january-6-2023