

THREAT INTEL INSIGHTS

OCTOBER 2023



1

MICROSOFT USERS TARGETED BY EVILPROXY PHISHING KIT EXPLOITING INDEED.COM VULNERABILITY

A newly discovered phishing campaign set its sights on the Microsoft 365 accounts of important executives within the U.S.-centered organizations. This malicious campaign abuses open redirects originating from the Indeed employment website, which is typically used for job listings. This campaign is facilitated by the use of the EvilProxy phishing service, which is adept at collecting session cookies that can be used to bypass multi-factor authentication systems. The primary targets of this campaign are high-level executives across various industries, including banking, manufacturing, real estate, finance, insurance, and property management.

2

THOUSANDS OF ANDROID DEVICES SOLD WITH BACKDOORED FIRMWARE

Researchers discovered a worldwide network of products called BADBOX that have firmware backdoors installed and are being shipped through an infected hardware supply chain. There are at least 74,000 Android phones, tablets, and TV boxes with the backdoored firmware being sold globally. Some of these products have been discovered on public school networks in the U.S. A compromised supply chain of a Chinese manufacturer was identified to be involved in the backdooring of firmware of multiple products, which are then supplied to resellers, e-commerce warehouses, and physical retail stores.

3


ZERO-DAY VULNERABILITY 'HTTP/2 RAPID RESET' EXPLOITED TO LAUNCH RECORD-BREAKING DDOS ATTACKS

A new distributed denial of service (DDoS) attack technique known as 'HTTP/2 Rapid Reset' has been actively exploited as a zero-day vulnerability since August. This technique has shattered previous records in terms of the scale of the attacks. Major internet infrastructure providers, including Amazon Web Services, Cloudflare, and Google, have come together to report their efforts in mitigating these attacks. The vulnerability exploited in these attacks has been tracked as CVE-2023-44487, carrying a CVSS score of 7.5 out of 10, signifying its severity. Amazon reported mitigating attacks reaching 155 million requests per second, Cloudflare handled 201 million rps, and Google astonishingly faced an attack of 398 million rps. Google managed to thwart these attacks by enhancing the capacity of their network's edge.

4

MIDDLE EAST GOVERNMENT NETWORK TARGETED BY IRANIAN APT OILRIG IN 8-MONTH CAMPAIGN

OilRig (APT34), the Iranian hacking group, successfully infiltrated a Middle Eastern government network, compromising a minimum of twelve computers and maintaining undetected access for a period spanning eight months from February to September 2023. The threat actors were able to steal a large number of files and passwords, as well as deployed a PowerShell backdoor called PowerExchange. Researchers tracked the campaign by the name Crambus. The actors used the implant to observe incoming mails sent from an exchange server so they could execute commands in the form of emails.



5

LAZARUS GROUP UTILIZES TROJANIZED VNC APPS TO TARGET DEFENSE EXPERTS WITH FAKE INTERVIEWS

The North Korean APT group Lazarus (aka Hidden Cobra) was observed using trojanized Virtual Network Computing (VNC) app versions to lure nuclear engineers and target the defense industry as part of their persistent campaign dubbed as Operation Dream Job. Operation Dream Job alludes to a series of attacks organized by the North Korean APT group in which their potential targets are contacted through suspicious accounts using multiple different social media platforms like Telegram, LinkedIn, and WhatsApp by pretending to offer job opportunities in order to trick them into installing the malware. Threat actor tricks job seekers into opening malicious apps for fake job interviews. To avoid detection by behavior-based security solutions, these backdoored application operates discreetly, only activating when the user selects a server from the drop-down menu of the Trojanized VNC client.

6

CISCO ALERTS ABOUT ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN IOS XE SOFTWARE

A warning issued by Cisco about a new critically severe authentication bypass zero-day vulnerability in its IOS XE software, which is actively being exploited and allows unauthenticated users to gain full administrator privileges, allowing attackers to take full remote control of infected switches and routers. The flaw is tracked as CVE-2023-20198, affecting devices that are running with the Web User Interface feature enabled while also having the HTTP or HTTPS Server feature turned on. According to the researchers, Cisco identified active exploitation of a previously unknown vulnerability in the Web User Interface (Web UI) feature of Cisco IOS XE software when exposed to the internet or untrusted networks.

7

STAYIN' ALIVE CAMPAIGN LINKED TO CHINA TARGETS ASIAN TELECOM AND GOVERNMENT ORGANIZATIONS

Since 2021, a persistent cyber campaign named “Stayin’ Alive” has been actively targeting high-profile government and telecom entities across Asia. This campaign aims to deploy basic backdoors and loaders as a means to deliver more advanced malware in subsequent stages. Researchers have been monitoring this campaign, which has targeted organizations in countries such as Vietnam, Uzbekistan, Pakistan, and Kazakhstan. The tools used in the Stayin’ Alive campaign are characterized by their simplicity and a wide range of variations. These tools appear to be disposable and are primarily used to download and execute additional malware payloads. Notably, these tools do not share any clear code similarities with known threat actors and lack significant commonalities among themselves.

8

MALICIOUS CAMPAIGN DISTRIBUTING HUNDREDS OF INFO-STEALING PYTHON PACKAGES

Researchers discovered a malicious campaign that has grown significantly over the past six months in which threat actors distributed hundreds of malicious packages on open-source platforms, having up to 75,000 downloads. This campaign has been observed since early April and researchers discovered 272 packages of malicious code used to steal sensitive information from the victims. The threat has evolved a lot since the time it was first identified, and the threat actors have implemented many sophisticated techniques to evade detection. A particular pattern has been noticed within the Python ecosystem since early April 2023, like the “_init_py” file loading only after it checks whether its on a virtual system or not, which is a common sign of malware presence.