Trading Accounts Targeted by WinRAR Zero-Day

WinRAR is one of the most popular compression tools with over 500 million users worldwide. Active since April 2023, the WinRAR zero-day vulnerability allows threat actors to create malicious files within .RAR and .ZIP archives. By spoofing harmless file formats such as JPG images, text files, or PDF documents, when opened, the flaw caused a script to execute installation of malware on the device. Group-IB was the first to discover the vulnerability and **released a report on 23 August**. They found that this vulnerability was being used to target cryptocurrency and stock trading forums, where the threat actors would post links to the WinRAR ZIP or RAR archives pretending to be trading strategies. While they cannot confirm the total number of infected devices, it is known that at least 130 traders' devices are still infected. After infecting the devices, the actors withdrew money from the broker accounts. The vulnerability has been posted as CVE-2023-38831 and it is highly recommended that all users install the latest version of WinRAR.

New Actively Exploited Ivanti Sentry Zero-Day Vulnerability

On 21 August, **Ivanti released information** on a new vulnerability that was discovered for Ivanti Sentry (formerly MobileIron Sentry). The vulnerability enables an unauthorized actor to access sensitive APIs which are used on the administrator portal to configure Ivanti Sentry. If successful, the actor can change configuration, run system commands, or write files to the system. This can be accomplished if the actor bypasses "authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration." If you do not expose port 8443 to the internet, there is a low risk of exploitation.

FBI Urges Immediate Removal of Network Device

On 23 August 2023, the US Federal Bureau of Investigation (FBI) urged **firms to remove Barracuda Network's Email Security Gateway (ESG)** appliances due to an independently verified exploit (**CVE-2023-2868**) to these products. The issue is a **backdoor vulnerability reported by CISA** used by malicious actors to insert malicious payloads onto the ESG appliance with different capabilities that include persistent access, emails scanning, credential harvesting and data exfiltration. The FBI has strongly advised all affected ESG appliances to be isolated and replaced immediately, and all networks to be scanned for connections to a provided list of indicators of compromise.

Suspected Chinese hackers in a state-run cyberespionage operation have exploited the vulnerability in the appliance to compromise hundreds of firms. Researchers from Mandiant determined with high confidence in June 2023 attackers had begun to **exploit the zero-day** last October and earlier. Barracuda applied a security patch in late May after observing attacks which allows hackers to send a malicious file resulting in a command injection to the appliance. Hackers responded to Barracuda's patch by modifying its primary backdoor to evade detection, which resides in the SQL database on the appliance.

NIST Provides Draft Update of its Cybersecurity Framework

On 8 August, **NIST released** its public draft of the NIST Cybersecurity Framework (CSF) 2.0. This is the first major update to the framework since 2014 and it includes a wider array of organizations, including small and medium-sized businesses, local schools and other entities, compared to only addressing critical infrastructure in the first iteration. Additionally, it has more focus on cybersecurity governance, the increasing risk of third-parties, and supply chain cybersecurity. The governance piece is added as a sixth function of the framework, which previously had five main functions: how to identify, protect, detect, respond and recover from cyberattacks or data breaches. A reference tool for the CSF 2.0 will be released in the coming weeks to help with browse, search, and export data in a machine-readable format.

Account Takeover Scheme Targeted Executives of Over 100 Global Organizations

The phishing tool named EvilProxy was used by threat actors to send 120,000 phishing emails to over one hundred global organizations with a goal of stealing their Microsoft 360 accounts. The EvilProxy tool allows attackers to steal MFA-protected credentials and session cookies. **Proofpoint** reported an increase of over 100% in successful cloud account takeover incidents in the past six months impacting high-level executives of these companies. They specifically targeted C-level executives, most of whom were Chief Financial Officers, Presidents, and CEOs. Additionally, they focused their efforts on personnel with access to financial assets or sensitive information.

The phishing email used brand impersonation, scan blocking, and a multi-step infection chain to compromise the accounts. Once compromised, the attackers leveraged a native Microsoft 365 application to execute MFA manipulation. They added their own MFA method to continue with access to the account. The threat actors were then seen committing financial fraud, data exfiltration, or selling access to the compromised accounts.

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.