rewterz

2023

THREAT INTEL INSIGHTS

JULY 2023

1

MALVERTISING CAMPAIGN: BLACKCAT RANSOMWARE OPERATORS SPREADS RANSOMWARE DISGUISED AS WINSCP

The BlackCat ransomware group, also known as ALPHV, has been conducting malvertising campaigns to deceive users into visiting fake websites that mimic the official WinSCP file-transfer application's website. WinSCP is a widely used SFTP, FTP, S3, SCP client, and file manager for Windows. BlackCat uses this legitimate software as a lure to target system administrators, web admins, and IT professionals, aiming to gain initial access to valuable corporate networks. The malicious ads promoting the fake WinSCP pages were found on both Google and Bing search pages.

2

CLAIM BY ANONYMOUS SUDAN: ALLEGED ACCESS TO 30 MILLION MICROSOFT ACCOUNTS

In June 2023, Microsoft experienced significant service outages, affecting Outlook email, OneDrive file-sharing apps, and the Azure cloud computing infrastructure. The responsibility for these DDoS attacks was claimed by a group known as Anonymous Sudan. However, in July, Anonymous Sudan made an announcement claiming to have stolen credentials for 30 million Microsoft customer accounts. They published a message on their Telegram channel, declaring a successful hack of Microsoft and offering a large database containing the alleged stolen data for sale at a price of $50,000.

3

REDENERGY: ADVANCED STEALER-AS-A-RANSOMWARE TARGETS ENERGY AND TELECOM SECTORS

RedEnergy is a newly discovered cyber threat known as a "Stealer-as-a-Ransomware" deployed in targeted attacks against energy utilities, oil, gas, telecom, and machinery sectors. This sophisticated malware enables the attackers to extract sensitive information from different web browsers and possesses the ability to function as ransomware. Researchers highlight that the RedEnergy malware employs a deceptive campaign, "FAKEUPDATES", to trick victims into updating their web browsers. Once inside the system, the malware stealthily extracts sensitive information and proceeds to encrypt the compromised files. The threat actors behind RedEnergy have been using reputable LinkedIn pages to target victims, including a machinery manufacturing company in the Philippines and multiple organizations in Brazil.

4

AUTHORITIES RAISE CONCERNS OVER ESCALATING TRUEBOT MALWARE ATTACKS

Cybersecurity agencies issued warnings about the emergence of new variants of the TrueBot malware, which is targeting companies in the U.S. and Canada. This sophisticated threat leverages a critical vulnerability (CVE-2022-31199) found in the widely used Netwrix Auditor server and its associated agents. Exploitation of this vulnerability grants unauthorized attackers the ability to execute malicious code with SYSTEM user privileges, providing them unrestricted access to compromised systems. TrueBot malware, associated with cybercriminal collectives Silence and FIN11, aims to extract confidential data and distribute ransomware, posing a significant risk to infiltrated networks.

5

TEAMSPHISHER TOOL EXPLOITS MICROSOFT TEAMS TO DEPLOY MALWARE

A new tool called “TeamsPhisher” has been made available on GitHub, allowing attackers to exploit a recently disclosed vulnerability in Microsoft Teams. This tool is designed to deliver malicious files to targeted Teams users within an organization. It specifically works in environments where internal Teams users can communicate with external users or tenants. The tool exploits a vulnerability highlighted by a security services company. TeamsPhisher automates the attack process, utilizing techniques from various sources and verifying the target’s ability to receive external messages.

6

WINDOWS AND MACOS SYSTEMS TARGETING BY AN IRAN-LINKED APT; TA453

TA453, a nation-state threat actor also known as Charming Kitten, PHOSPHORUS, and APT42, has been identified in a recent malware campaign targeting both Windows and macOS systems. This campaign marks a shift in TA453's tactics as they have started using LNK infection chains instead of Microsoft Word documents with macros. The initial attack vector involves spear-phishing emails that pose as benign conversations, impersonating a senior fellow from the Royal United Services Institute (RUSI) to a public media contact at a US-based think tank focused on foreign affairs.

7

DISCOVERY OF A NEW CRITICAL UNAUTHENTICATED SQL INJECTION VULNERABILITY IN MOVEIT TRANSFER SOFTWARE

Progress Software announced a significant security development regarding their widely used secure file transfer software, MOVEit Transfer. The company has successfully identified and patched a critical SQL injection vulnerability, specifically tagged as CVE-2023-36934. This vulnerability represents a severe security flaw that has the potential to grant unauthorized access to the MOVEit Transfer database, even for unauthenticated attackers. By exploiting this particular vulnerability, attackers can send specially crafted payloads to specific endpoints within the affected application, thus altering or exposing sensitive data stored within the database.

8

BANKING SECTOR TARGETED IN OPEN-SOURCE SOFTWARE SUPPLY CHAIN ATTACKS

Researchers made a significant discovery, identifying what appears to be the first open-source software supply chain attacks specifically aimed at the banking sector. The attackers utilized advanced techniques, including focusing on specific components within the web assets of victim banks by attaching malicious functionalities to them. The attackers employed deceptive tactics, including creating a fake LinkedIn profile to appear credible and customizing command-and-control (C2) centers for each target. By exploiting legitimate services, they managed to carry out their illicit activities effectively. The malicious npm packages used in these attacks were later reported and taken down, although their names were not disclosed.