rewterz

2024

THREAT INTEL INSIGHTS

JANUARY 2024

1

KASSEIKA RANSOMWARE DISABLES ANTIVIRUSES BY LEVERAGING BYOVD ATTACKS

A newly discovered ransomware operation dubbed “Kasseika" was seen deploying Bring Your Own Vulnerable Driver (BYOVD) attacks to encrypt files after disabling antivirus software. The ransomware exploits the Martini driver, part of TG Soft’s VirtIT Agent System, to disable the security solutions protecting the targeted machine. It was found that this ransomware strain has many similar features to BlackMatter, like attack chains and source code. BlackMatter’s source code was never leaked in public after it shut down in 2021. Still, it seems likely that Kasseika was developed by the former members of the threat group or sophisticated ransomware actors who bought its code.

2

CLOUD AND SAAS PLATFORMS TARGETED BY NEW PYTHON-BASED FBOT MALWARE

A novel Python-based hacking toolkit dubbed FBot emerged targeting cloud services, web servers, content management systems (CMS), and SaaS platforms like Microsoft 365, Amazon Web Services (AWS), Twilio, and SendGrid. FBot is the newest addition to the list of tools that are used for hijacking cloud such as GreenBot (aka Maintance), AlienFox, Predator, and Legion. Researchers detailed some of the notable features of the malware including AWS account hijacking tools, credential harvesting to use in spamming attacks, and functions that enable attacks against PayPal and numerous SaaS accounts. FBot is described as related to these malware families but still distinct, as it doesn't use any source code from AndroxGh0st and only shares some similarities with Legion.

3

MEDUSA RANSOMWARE GANG ATTACKED 74 ORGANIZATIONS AFTER EXTORTION MODEL SWITCH

The operators of Medusa ransomware have increased their activities since the launch of their own data leak website on the dark web back in February 2023 where they post sensitive data stolen from victims who do not agree to their demands and refuse to pay ransom. About 74 organizations are estimated to have been hit by this ransomware in 2023, mostly in the U.K., the U.S., Italy, France, India, and Spain. This group has moved to rely on a multi-extortion strategy and will provide the victims with many options like time extension, data deletion, or downloading all data after the stolen information is posted on their leak website. All the options have a price tag that depends on the kind of organization impacted by the ransomware.

4

SAUDI ARABIAN MINISTRY EXPOSED SENSITIVE DATA FOR 15 MONTHS

The Ministry of Industry and Mineral Resources (MIM) of Saudi Arabia had an environment file that exposed sensitive information for anyone to access. Researchers believe that the sensitive data had been accessible for 15 months. An environment (env.) file is a critical system component used to convey a set of instructions to applications. These files expose sensitive data if left open for anyone to access and let threat actors have the ease to perform various malicious activities. The now-secured MIM's env. file exposed critical information that cybercriminals could leverage for lateral movement inside the ministry's systems and potentially doing anything from account takeover to a ransomware attack.

5

4.5 MILLION PATIENTS IMPACTED DUE TO HEALTHCARE TECH COMPANY DATA BREACH

A health management solutions provider, HealthEC LLC, suffered a data breach that has impacted almost 4.5 million patients who received healthcare from one of the company's customers. On 22nd December 2023, the company reported a data breach on July 14 and 23, resulting in unauthorized access to some of its systems. HealthEC is responsible for providing services through a population health management (PHM) platform that is used by healthcare organizations for data analytics, integration, patient engagement, care coordination, reporting, and compliance. The investigation of the incident was concluded on 24th October, revealing that the threat actor managed to steal sensitive files from the impacted systems including Name, Address, Date of birth, Social Security number, Taxpayer Identification Number, Medical Record number and other Medical and health insurance information.

6

CYBERCRIMINALS EXPLOIT OFFICIAL AND CORPORATE ACCOUNTS ON X TO CARRY OUT CRYPTO FRAUDS

Threat attackers are increasingly targeting verified accounts on X, the platform formerly known as Twitter. These accounts, marked with ‘gold’ and ‘grey’ check marks, are associated with government and business profiles, making them particularly attractive to cybercriminals. The attackers exploit these verified accounts to promote cryptocurrency scams, phishing sites, and crypto-draining schemes. A notable incident involved the X account of Mandiant, a cyber threat intelligence company and subsidiary of Google, which was recently hijacked. The attackers utilized the compromised account to distribute a fake airdrop, depleting cryptocurrency wallets. This incident is even more puzzling because Mandiant had two-factor authentication enabled on the account.

7

RUSSIAN THREAT ACTORS BREACHED UKRAINIAN TELECOM OPERATOR AND WIPED THOUSANDS OF SYSTEMS

Russian-linked threat actors who breached Kyivstar, Ukraine's largest telecommunications service provider, wiped thousands of systems on the main network of the telecom operator. The incident left about 25 million of the company's mobile and home internet subscribers without an internet connection. The attackers breached Kyivstar's network back in May 2023 as discovered by Ukrainian cybersecurity researchers. They launched the attack months after the initial breach and wiped all of the virtual servers and computers, destroying the core of the telecoms operator. The Ukrainian security company was able to prevent multiple attempts to cause more damage to the operator.

8

TRICKMO 2.0: THE REVIVAL: A RESURGENT BANKING TROJAN WITH ADDITIONAL FEATURES

The notorious banking Trojan, TrickBot, has resurfaced with a new Android variant known as “TrickMo,”. Initially detected in September 2019, TrickMo has evolved, utilizing JsonPacker to conceal its code. Unlike earlier versions, the latest TrickMo boasts enhanced capabilities, including overlay injection—a more sophisticated technique compared to traditional screen recording for capturing sensitive information. Overlay Attack allows TrickMo to efficiently carry out activities like exfiltrating device screen content, downloading runtime modules, and executing overlay attacks on targeted banking apps and browsers. This represents a notable advancement in TrickMo’s tactics since its inception, showcasing a more evolved and potent threat.