rewterz

2023

THREAT INTEL INSIGHTS

NOVEMBER 2023

1

NORTH KOREAN-BASED APT38 TARGETS IT JOB SEEKERS

Sapphire Sleet, a North Korean APT group affiliated with Lazarus, is known for targeting banks, venture capital firms, and cryptocurrency exchanges. Microsoft researchers issued a warning regarding the group's new social engineering tactics, involving fraudulent talent evaluation websites. The threat actor, specializing in cryptocurrency theft through social engineering, shifted its tactics by creating deceptive skills assessment portals. The group initially establishes contact using platforms like LinkedIn and then transitions to other channels such as email or messaging apps. Microsoft suspects that Sapphire Sleet adopted this new approach, including building its own websites, after identifying and adapting to the APT group's previous methods.

2

OKTA WARNS ABOUT 5,000 EMPLOYEES HAVING DATA EXPOSED AFTER HACKING OF THIRD-PARTY VENDOR

Okta, a cloud identity and access management solutions provider, disclosed about a data breach suffered by a third-party vendor Rightway Healthcare, resulting in nearly 5,000 of Okta's employees having their personal information exposed. According to the data breach notification, Okta was told by Rightway Healthcare that an unauthorized user gained access to an eligibility census file that was maintained by the provider as a service to Okta. Okta immediately launched an investigation to review the affected file in order to see how far it impacted the employees.

3

LOCKBIT RANSOMWARE ATTACKS KYOCERA AVX AND IMPACTS 39,000 INDIVIDUALSCE

A data breach at Kyocera AVX Components Corporation (KAVX) has exposed the personal data of 39,111 individuals after a LockBit ransomware attack. KAVX is a manufacturer of advanced electronic components in America, and a subsidiary of the Japanese semiconductor company Kyocera. It has over ten thousand employees with an annual revenue of $1.3 billion. The company sent out a notification talking about the data breach to the affected people, saying that the breach was discovered on 10th October, 2023 and the attackers had access to the systems between 16th February and 30th March of this year.

4

MIDDLE EASTERN GOVERNMENTS TARGETED IN PHISHING CAMPAIGNS WITH IRONWIND MALWARE

A new phishing campaign is targeting governments in the Middle East and is distributing an initial access downloader called IronWind. It was detected between July and October 2023, and researchers attributed it to a threat actor tracked as TA402. TA402 is a Middle Eastern advanced persistent threat (APT) group that has always proven to be a highly sophisticated group for cyber espionage that focuses on collecting intelligence. It constantly updates the IronWind malware's delivery mechanisms, like using XLL file attachments, Dropbox links, and RAR archives. Using IronWind is a big shift from TA402's previous attack chains, which utilized the use of a backdoor dubbed as NimbleMamba that also targeted Middle Eastern governments and foreign policy think tanks.

5

FASHION INDUSTRY PROFESSIONALS TARGETED BY DUCKTAIL MALWARE'S NEWEST CAMPAIGN

Ducktail's latest campaign focuses on targeting marketing professionals within the fashion industry, in which the attackers distribute archives that contain several images of real products from known brands, but it comes alongside a malicious executable disguised as a PDF file. When the malware is executed, it opens a genuine embedded PDF that has details on job information, specially crafted to appeal to the marketing professionals who are actively searching for new jobs. The malware's goal is to install a browser extension that is capable of stealing Facebook business and ad accounts, and later sell the stolen credentials to third parties.

6

RUSSIAN THREAT ACTORS LAUNCH THE LARGEST CYBER ATTACK ON DANISH CRITICAL INFRASTRUCTURE

In May 2023, cybercriminals with suspected ties to Russia executed a major attack on Denmark's critical infrastructure, affecting 22 energy-related companies. The attackers, believed to be associated with Russia's GRU military intelligence agency, Sandworm, exploited a critical vulnerability (CVE-2023-28771) in Zyxel firewalls, scoring 9.8 on CVSS. This flaw enabled a command injection, compromising industrial control systems of the targeted companies. Denmark's cybersecurity researchers reported that the affected companies had to implement island mode operation to mitigate the impact. The evidence linking the attacks to Sandworm includes traced IP addresses used in the campaign.

7

RECENT ‘HRSERV.DLL’ WEB SHELL DETECTED IN APT ATTACK TARGETING AFGHAN GOVERNMENT

An undisclosed Afghan government entity faced an advanced persistent threat (APT) attack involving a novel web shell named HrServ.dll. This dynamic-link library (DLL) showcases sophisticated features, including custom encoding for client communication and in-memory execution, according to the researcher. The Russian cybersecurity firm detected malware variants dating back to early 2021 based on compilation timestamps. Web shells, like HrServ.dll, are malicious tools granting remote control over compromised servers, enabling post-exploitation activities such as data theft, server monitoring, and lateral movement within networks.

8

FBI AND CISA ALERT ABOUT RHYSIDA RANSOMWARE ATTACKS ACROSS MULTIPLE SECTORS

The perpetrators of the Rhysida ransomware are involved in opportunistic attacks that focus on organizations across diverse industry sectors. CISA and the FBI have recently published a joint advisory that warns of increasing attacks by this ransomware gang. The Rhysida ransomware gang has been active since at least May 2023 and has impacted at least 62 companies since then, according to their website. The group is known for targeting organizations in multiple industries, some of which include the healthcare, education, manufacturing, government, and information technology sectors.