rewterz

2023

THREAT INTEL INSIGHTS

JUNE 2023

1

NORTH AFRICA TARGETED BY A NEW CUSTOM BACKDOOR "STEALTH SOLDIER"

An espionage campaign in North Africa has raised concerns as a new custom backdoor called “Stealth Soldier” has been deployed. The campaign involves highly-targeted attacks and is characterized by the use of command-and-control (C&C) servers that mimic websites belonging to the Libyan Ministry of Foreign Affairs. According to a technical report, the earliest artifacts associated with the campaign date back to October 2022. The Stealth Soldier malware is described as an undocumented backdoor that primarily focuses on surveillance functions. It is capable of performing various malicious activities, including file exfiltration, screen and microphone recording, keystroke logging, and stealing browser information

2

THREAT ACTORS ASSOCIATED WITH THE CYCLOPS RANSOMWARE OFFERING AN INFORMATION STEALER MALWARE TO CYBERCRIMINALS

Researchers reported that the notorious Cyclops ransomware gang has started offering a Go-based info stealer to other cybercriminals. This tool can be used to steal sensitive information such as login credentials, credit card details, and other personal data from infected hosts. The group is known for using advanced techniques to evade detection and encryption to lock victims' files. With this new offering, the Cyclops gang is expanding its reach and potentially increasing the number of victims it can target.

3

SWISS RAILWAY COMPANY FSS AFFECTED BY XPLAIN DATA BREACH: EXPANDED IMPACT OF THE CYBERATTACK

In early June, the IT services provider Xplain, based in Bern, Switzerland, experienced a Play ransomware attack that had a more significant impact than initially anticipated. The attack not only affected Xplain, but also targeted the national railway company of Switzerland (FSS) and the canton of Aargau. Swiss police launched an investigation into the incident. The news of the attack was first reported by a Swiss newspaper, which highlighted that several cantonal police forces, the Swiss army, and the Federal Office of Police (Fedpol) were indirectly impacted by the cyberattack. These entities shared a common IT service provider, Xplain, which had been hacked. Threat actors initially published alleged stolen data from Fedpol and the Federal Office for Customs and Border Security (FOCBS) on a Darknet forum.

4

BLACKSUIT ENCRYPTOR BOLSTERS THE ARSENAL OF THE ROYAL RANSOMWARE GANG

The Royal ransomware gang began testing a new encryptor called BlackSuit, which shares many similarities with the operation's usual encryptor. BlackSuit is a new ransomware family that was first discovered in May 2023, and it has been found to be significantly similar to the Royal ransomware family. The similarities between the two ransomware strains have led researchers to speculate that BlackSuit is either a new variant developed by the same authors, a copycat using similar code, or an affiliate of the Royal ransomware gang that has implemented modifications to the original family.

5

A CHINA-LINKED APT GROUP EXPLOITING A ZERO-DAY VULNERABILITY IN VMWARE ESXI

Researchers discovered a cyber espionage group known as UNC3886, which is believed to be sponsored by China, exploiting a zero-day vulnerability in VMware ESXi. The vulnerability, tracked as CVE-2023-20867, allowed the group to backdoor Windows and Linux virtual machines hosted on compromised ESXi hosts. The attackers leveraged a VMware Tools authentication bypass flaw to deploy VirtualPita and VirtualPie backdoors, gaining root privileges on the guest VMs. By using maliciously crafted vSphere Installation Bundles (VIBs), the group installed the backdoor malware on the ESXi hosts.

6

JOKERSPY BACKDOORS AND SPYWARE TARGET APPLE MACOS SYSTEMS

Researchers uncovered a sophisticated toolkit specifically designed to target Apple macOS systems, revealing a concerning threat to Mac users' security. The toolkit, which has been largely undetected so far, consists of malicious artifacts that have been analyzed by experts. The analysis is based on four samples that were uploaded to VirusTotal by an unidentified victim. The earliest sample dates back to April 18, 2023, indicating that this threat has been active for several months without significant detection.

7

PAKISTANI INDIVIDUALS TARGETED IN ADVANCED ESPIONAGE CAMPAIGN THROUGH MALICIOUS ANDROID APPS

Individuals in the Pakistan region have been targeted using two rogue Android apps available on the Google Play Store as part of a new targeted campaign. The campaign has been attributed to a threat actor known as DoNot Team or APT-C-35. The main objective of this attack is to collect personal data from unsuspecting victims by disguising a malicious program as a legitimate app. The extracted information, including contact details and location data, is likely intended for future attacks involving more destructive malware.

8

GEN DIGITAL CONFIRMS EMPLOYEE DATA BREACH IN MOVEIT RANSOMWARE ATTACK

Gen Digital Inc., the parent company of Norton, has fallen victim to a ransomware attack that targeted the recently disclosed MOVEit zero-day vulnerability. Gen Digital is a multinational software company specializing in cybersecurity software and services, owning brands such as Norton, Avast, LifeLock, Avira, AVG, ReputationDefender, and CCleaner. The attack leveraged the MOVEit Transfer vulnerability (CVE-2023-34362) which is a SQL injection vulnerability in the managed file transfer system used by enterprises for secure file transfers via SFTP, SCP, and HTTP-based uploads. The Clop ransomware group, also known as Lace Tempest, has claimed responsibility for the attack and has been credited by Microsoft for exploiting the zero-day vulnerability.