

THREAT INTEL INSIGHTS

MAY 2023



1

NORTH KOREAN APT KIMSUKY LAUNCHES GLOBAL SPEAR-PHISHING CAMPAIGN

The Kimsuky hacking group, aka Thallium and Velvet Chollima, is a state-sponsored cyberespionage group that has been active since at least 2012. The group was observed using a new version of its reconnaissance malware, called ReconShark (an evolution of the threat actor's BabyShark malware toolset), in a global cyberespionage campaign. The malware is designed to gather information on targeted systems and exfiltrate that data back to the attackers. It is believed that the group uses this information to gain access to sensitive networks and steal valuable intellectual property.

2


NEW CACTUS RANSOMWARE EXPLOITS VPN FLAWS TO INFILTRATE NETWORKS

A new ransomware operation, Cactus, has been observed exploiting vulnerabilities in VPN appliances to get early access to targeted networks. This new strain leverages known vulnerabilities to gain initial access to targeted networks and then utilizes custom scripts to automate the deployment and detonation of the ransomware encryptor. The double extortion tactics used by CACTUS actors add an additional layer of threat to organizations, as they not only face the potential loss of encrypted data but also the exposure of sensitive data stolen prior to encryption.

3

STORMKITTY STEALER: A THREATENING INFORMATION-STEALING MALWARE

StormKitty information stealer is designed to compromise sensitive data from infected systems, such as login credentials, passwords, cryptocurrency wallets, and other valuable information. The stolen data is often used for various malicious purposes, including identity theft, financial fraud, and unauthorized access. StormKitty Stealer incorporates anti-analysis techniques to evade detection by security software. This includes obfuscating code, employing packers or encryptors, and detecting the presence of virtual machines or sandboxes. The malware can be distributed as an email attachment disguised as a legitimate file, such as a PDF, Word document, or an archived file.



4

APT SIDEWINDER GROUP TARGETING VICTIMS IN PAKISTAN AND TURKEY USING SERVER-BASED POLYMORPHISM TECHNIQUE

SideWinder, an advanced persistent threat (APT) actor, has been accused of using a backdoor in attacks targeting Pakistan government organizations as part of a campaign that began in late November 2022. The APT group uses a server-based polymorphism technique to deliver the next stage payload, which makes it harder for security software to detect and block the malware. Server-side polymorphism is a technique used by threat actors and other distributors of malware to evade detection by antivirus scanners.

5

A THREAT FROM THE SHADOWS OF LOKILOCKER, BLACKBIT RANSOMWARE BEING DISTRIBUTED IN KOREA

According to researchers, BlackBit ransomware is identified as a variant of LokiLocker ransomware and operates on the Ransomware-as-a-Service (RaaS) model. The source code analysis of BlackBit suggests that it is a copy of LokiLocker with cosmetic changes such as icons, names, and color schemes. These modifications may have been made to differentiate BlackBit from its original counterpart and potentially confuse security researchers.



6

BARRACUDA ISSUES WARNING REGARDING ZERO-DAY EXPLOITATION TO BREACH EMAIL SECURITY GATEWAY (ESG) APPLIANCES

An email protection and network security services provider issued a warning regarding a zero-day vulnerability that has been exploited to compromise their Email Security Gateway (ESG) appliances. According to Barracuda, their security solutions are utilized by over 200,000 organizations worldwide. The zero-day vulnerability tracked as CVE-2023-2868 is classified as a remote code injection vulnerability. It affects Barracuda Email Security Gateway appliances running versions 5.1.3.001 through 9.2.0.006.

7

THREAT ACTORS WEAPONIZING .ZIP DOMAINS TO TRICK VICTIMS

Researchers discovered an advanced phishing method called “file archiver in the browser” that exploits .ZIP domains to deceive unsuspecting individuals. This technique impersonates a file archiver software within a web browser when someone visits a website with a .ZIP domain. The attackers create a fraudulent webpage that closely resembles legitimate file archiving software, utilizing HTML and CSS to imitate the interface and design elements. By hosting this deceptive page on a .ZIP domain, they aim to enhance the credibility of their social engineering campaigns.