

THREAT INTEL INSIGHTS

SEPTEMBER 2023



1

NEW ADVANCED BACKDOOR MALWARE DEADGLYPH UNCOVERED IN GOVERNMENT-TARGETED ATTACKS

In a recent cyberespionage incident in the Middle East, a highly advanced backdoor malware known as "Deadglyph" was employed. This malware is linked to a state-sponsored hacking group called Stealth Falcon APT, also known as Project Raven or FruityArmor, originating from the United Arab Emirates (UAE). The group has garnered a reputation for its activities over nearly a decade, primarily focusing on targeting individuals such as activists, journalists, and dissidents.

2


QR CODE PHISHING CAMPAIGN TARGETS PROMINENT U.S. ENERGY ORGANIZATION

One of the US's major energy companies was recently targeted by cybercriminals in a phishing campaign, where they used QR codes to transfer malicious phishing emails into target inboxes and bypass security. About 29% of the 1000 emails affected by this attack were victims of a notable energy company in the US, while the rest of the targeted emails were organizations in the manufacturing, technology, insurance, and financial sectors. Researchers note that this is the first time QR codes have been used in such a large-scale phishing campaign, warning that in the near future more threat actors may consider using it as their attack vector. The phishing email received in this campaign tricks the target user by claiming that they need to update their Microsoft 365 account settings urgently. There is a PNG or PDF attachment of a QR code in these emails that the target is urged to scan in order to verify their account.

3

CHINESE APT, EARTH LUSCA, ADOPTS SPRYSOCKS LINUX MALWARE TO BOLSTER ITS CYBER ARSENAL

Researchers have discovered an encrypted file hosted on a server while monitoring the Chinese malicious group Earth Lusca. This has led to the discovery of a Linux backdoor that was previously unknown, now tracked as SprySOCKS. The code is based on the open-source Windows backdoor called Trochilus, which has many of its functions rewritten so it can run on Linux systems. There have been two SprySOCKS samples detected with different versions, suggesting that the backdoor is still under development. The researchers think that the implementation of the interactive shell is probably based on the Derusbi malware, especially its Linux variant.



4

MICROSOFT ACCIDENTALLY LEAKS 38TB OF PRIVATE DATA THROUGH UNSECURED AZURE STORAGE

Microsoft acknowledged a significant security breach that exposed 38 terabytes of private data, which was discovered on the company's AI GitHub repository. This data leak occurred when a bucket of open-source training data was inadvertently made public. It included sensitive information such as secrets, keys, passwords, and over 30,000 internal Microsoft Teams messages, originating from two former employees' workstations.

5

EVILBAMBOO SPYWARE TARGETS TIBETANS, TAIWANESE, AND UYGHURS

The threat actor known as EvilBamboo has been conducting a sustained campaign aimed at gathering sensitive information, with a primary focus on individuals and organizations hailing from Tibet, Uyghur, and Taiwan.

Security researchers have discovered that EvilBamboo is behind the creation of fraudulent Tibetan websites and social media profiles, which are likely used to distribute browser-based exploits to their targeted victims. Furthermore, the attacker has established online communities on platforms like Telegram, often by impersonating existing popular groups, to facilitate the dissemination of their malicious software.

6

PAYMENT CARD-SKIMMING CAMPAIGN EXPANDS FOCUS TO NORTH AMERICAN WEBSITES

A new payment card skimming campaign called “Silent Skimmer” has been identified by researchers, and it is targeting online payment businesses in the Asia-Pacific (APAC) and North America and Latin America (NALA) regions. This campaign has been active for a year and is ongoing. Evidence suggests that Chinese actors are behind it, as the attacker is believed to be from the APAC region and proficient in the Chinese language. Silent Skimmer appears to be financially motivated. The attacker gains initial access by exploiting known vulnerabilities and compromised web servers. Ultimately, they deploy payment scraping tools on infected sites to steal sensitive financial data. Initially, the campaign primarily targeted companies in the APAC region. However, starting from October 2022, the attacker expanded their focus to include Canada and North America.



BLACKCAT/ALPHV RANSOMWARE GROUP ALLEGEDLY ENCRYPTED OVER 100 MGM ESXI SERVERS

An affiliate of the BlackCat ransomware group, also known as APLHV, recently carried out a significant cyberattack on MGM Resorts, leading to the disruption of the company's operations and the shutdown of its IT systems. The attack involved the infiltration of MGM's infrastructure, during which more than 100 ESXi hypervisors were encrypted by the attackers after the company had taken down its internal infrastructure. BlackCat claimed that they had exfiltrated data from MGM's network and maintained access to some parts of the infrastructure and threatened to launch further attacks unless a ransom agreement was reached with the company. The threat actor behind the MGM breach was also tracked by various cybersecurity companies under different names, including Scattered Spider, Oktapus, and UNC3944.

8

FAKE TELEGRAM APPS ON GOOGLE PLAY DISTRIBUTING SPYWARE ON ANDROID DEVICES

Multiple fake Telegram apps have been discovered on Google Play for Android that are infecting devices with spyware and are also capable of stealing messages, contact lists and other personal data. Most of these apps have been installed over 60,000 times. These malicious apps seem to be targeting Chinese-speaking users and the Uighur ethnic minority. The apps are promoted as “faster” alternatives to the regular Telegram, and seeing the number of installs, the campaign has been successful in reaching the potential targets. Analysts revealed that these apps appear identical to Telegram but contain extra code to steal data, including a package named ‘com.wsys’ that accessed contacts, usernames, user IDs, and phone numbers. The spyware sent copies of received messages to a command and control server. The exfiltrated data, encrypted before transmission, included message content, chat/channel details, sender information, and monitored changes to usernames and contact lists.