rewterz

2022

THREAT INTEL INSIGHTS

DECEMBER 2022

1

RUSSIA’S SECOND-LARGEST BANK VTB TARGETED BY A DDOS ATTACK

The second-largest financial institution in Russia, VTB Bank, suffered the worst cyberattack in its history after a Distributed Denial Of Service (DDOS) attack forced the closure of both its website and mobile apps. The bank claims that internal analysis shows that the DDoS attack was planned and orchestrated with the specific aim of disturbing the bank’s customers by interfering with their banking services.

2

CONFUCIUS APT GROUP TARGETING PAKISTAN GOVERNMENT

Confucius APT group, an Indian state-sponsored APT group, was observed targeting Pakistan Government and Military by delivering a new version of their “Print.dll” trojan with control flow obfuscation, with version ID 3.1.0. The group’s main target is Pakistan and other South Asian countries. Previously, the group used mobile malware to infiltrate its victims. Android surveillanceware tools like SubBird, ChatSpy, and Hornbill have been used by the group to spy on the victims.

3

SHUCKWORM APT GROUP'S PHISHING CAMPAIGN TARGETED SECURITY SERVICES IN UKRAINE

Shuckworm APT – aka Actinium, Armageddon, Primitive Bear, Gamaredon, and Trident Ursa – is a Russia-backed advanced persistent threat (APT) that has been operating since at least 2013. In December, this APT group conducted a phishing campaign against the Security Services of Ukraine (http://ssh.gov.ua) with the email subject regarding the corruption of SBU military accounting documents

4

BITCOIN MINING POOL BTC.COM LOST $3M WORTH OF CRYPTOCURRENCY IN CYBERATTACK

One of the biggest cryptocurrency mining pools in the world, BTC.com becomes the target of a cyberattack that resulted in the theft of around $3 million worth of crypto assets. BTC.com is one of the largest platforms for transferring Bitcoin, with millions of users worldwide. The cyberattack resulted in the theft of $2.3 million in digital assets owned by the company as well as $700,000 in cryptocurrency owned by customers of the company. The company reported the attack to Chinese law enforcement officials in Shenzen after discovering the attack. On December 23rd, 2022, the authorities initiated an investigation into the security breach.

5

NJRAT TARGETING YEMEN

NjRat was seen targeting Yemen in its latest campaign with the file related to Important leaked documents of the Houthi group. NjRat is a remote access trojan (RAT) with the ability to view the victim's desktop, upload/download files, log keystrokes, access the victim's camera, steal browser-stored credentials, open a reverse shell, perform processes, and allow the attacker to update, uninstall, restart, close, disconnect, and rename the RAT's campaign ID.

6

MUSTANG PANDA SPEAR-PHISHING CAMPAIGN

Researchers uncovered a large-scale phishing campaign aimed at the government, academic, foundation, and research sectors, with a focus on Australia, Japan, Taiwan, Myanmar, and the Philippines. In the campaign, Earth Preta exploited fake Google accounts to spread malware via spear-phishing emails, the malware was initially stored in an archive file (such as a rar/zip/jar file) and distributed through Google Drive links. Throughout the campaign, new malware families were utilized by the gang (TONEINS and TONESHELL), including PUBLOAD, a previously disclosed malware.