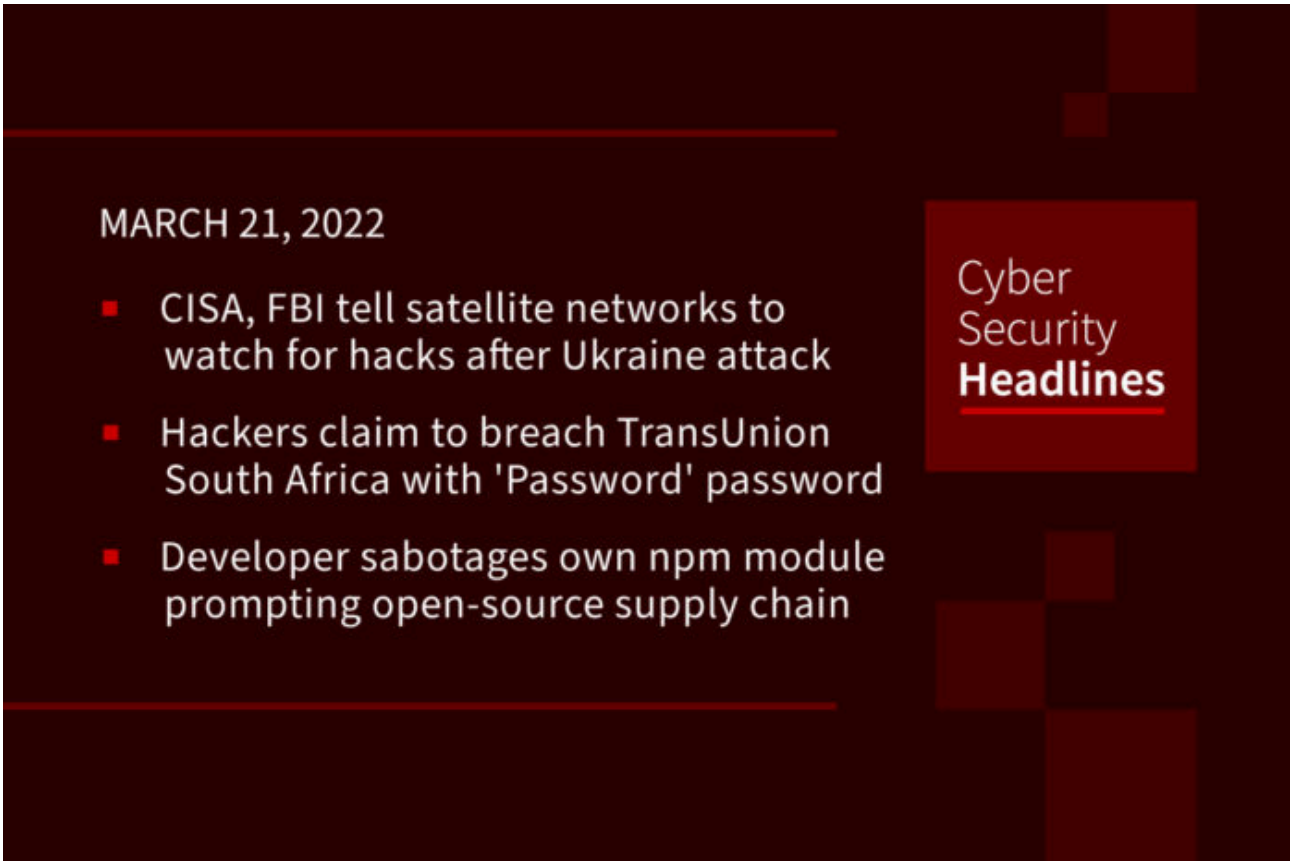
Cyber Security Headlines – March 21, 2022

By Steve Prentice

Published: 2022-03-21 · Archived: 2026-05-01 02:07:59 UTC



CISA, FBI tell satellite communications network owners to watch out for hacks after Ukraine attack

This alert forms part of CISA's "Shields Up" program which responds to potential Russian cyberattacks related to the Ukraine conflict. As part of the defense of SATCOM network, the program asks all organizations to "significantly lower their threshold for reporting and sharing indications of malicious cyber activity." As an example of the danger, Victor Zhora, the deputy chairman of the State Service of Special Communications and Information Protection of Ukraine, described to the media how the digital sabotage of Viasat's KA-SAT satellite hours before the Russian invasion led to "huge loss in communications in the very beginning of the war." As a consequence, lawmakers in the US are pressing the DHS to name space as another critical infrastructure sector like health care or energy.

(Cyberscoop)

Hackers claim to breach TransUnion South Africa with 'Password' password

Hackers have breached a server belonging to TransUnion South Africa and have demanded a ransom payment. The hacking group, “N4ughtysecTU” is based in Brazil, and says they downloaded 4TB of data. The group also told Bleeping Computer “they didn’t steal any user credentials but performed a brute force attack on the SFTP server. The account they ultimately breached was allegedly using the password “Password”, so it was quick and straightforward to brute-force.” TransUnion has noted it will not pay the ransom.

(Bleeping Computer)

Developer sabotages own npm module prompting open-source supply chain security questions

According to CSOOnline, the developer of a popular JavaScript component hosted on the npm repository “decided to protest Russia’s invasion of Ukraine by adding code to their own component that would add or delete files on people’s computers in a way they didn’t expect.” The component, node-ipc, is a dependency for a variety of other projects which consequently had to receive emergency updates to compensate. Experts believe that while developers certainly have the right to modify their own software, in an act of self-sabotage called protestware, “such acts risk damaging trust in the open-source ecosystem, which has faced increased supply-chain security challenges in recent years.”

(CSOOnline)

Cloud-based email threats surge 50% in 2021

This corresponds with a drop in ransomware and business email compromise (BEC) detections as attacks become more targeted, according to Trend Micro in a recent report. “The number of phishing attempts almost doubled during the period, as threat actors continued to target home workers. Of these, 38% were focused on stealing credentials, the report claimed.” The report also mentions that misconfigured cloud systems were also a critical risk factor in 2021, with AWS Key Management Service (AWS KMS) and Amazon Elastic Container Service (Amazon ECS) having some of the highest misconfiguration rates

(InfoSecurity Magazine)

Thanks to our episode sponsor, Varonis

Avoslocker ransomware gang targets US critical infrastructure

The FBI has published a joint cybersecurity advisory in conjunction with the US Treasury Department and the Financial Crimes Enforcement Network, warning of AvosLocker ransomware attacks targeting multiple US critical infrastructure. The AvosLocker ransomware-as-a-service emerged in the threat landscape in September 2021, and since January has expanded its targets by implementing the support for encrypting Linux systems, specifically VMware ESXi servers. AvosLocker claims to directly handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data after their affiliates infect targets.

(Security Affairs)

New Phishing toolkit lets anyone create fake Chrome browser login windows

According to BleepingComputer, “A phishing kit has been released that allows red teamers and wannabe cybercriminals to create effective single sign-on phishing login forms using fake Chrome browser windows, known as a Browser in the Browser (BitB) Attack.” Security researcher mr.d0x told BleepingComputer that these templates are easy to use in creating convincing Chrome windows to display single sign-on login forms for any online platform. Mr.d0x, who released the templates Google Chrome for Windows and Mac on GitHub, said that redteamers could simply download the templates, edit them to contain the desired URL and Window title, and then use an iframe to display the login form. “Kuba Gretzky, creator of the Evilginx phishing toolkit, tested the new method and showed how it worked perfectly with the Evilginx platform, meaning it could be adapted to steal 2FA keys during phishing attacks.”

(Bleeping Computer)

DarkHotel APT targets Wynn, Macao Hotels to steal guest data

The group has been targeting luxury hotels in Macao with a spear-phishing campaign aimed at “breaching their networks and stealing the sensitive data of high-profile guests staying at resorts.” A threat research report from Trellix identified the South Korean DarkHotel APT group as the culprit, stating the campaign began at the end of November. It consisted of with emails containing malicious Excel macros that were sent to members of hotel management who had access to hotel networks. These included human resources and office managers.

(ThreatPost)

Anonymous leaks data stolen from Russian pipeline company Transneft

According to Security Affairs, “the Anonymous collective claims it has hacked Omega Company, the in-house R&D unit of Transneft, the Russia-based state-controlled oil pipeline company.” The hacktivists claim to have stolen 79GB of emails from the largest oil pipeline company in the world, and havepublished them on the leak site of Distributed Denial of Secrets, a non-profit whistleblower organization. The stolen data includes invoices, equipment technical configurations, and product shipment information. The Omega Company produces high-tech acoustic and temperature monitoring systems for oil pipelines.

(Security Affairs)

Source: https://cisoseries.com/cyber-security-headlines-march-21-2022/