Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On October 14, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft and Adobe products. On October 13, the MS-ISAC released an advisory for multiple vulnerabilities in Microsoft products, the most severe of which could allow for remote code execution.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

16 October 2020

Other subjects of interest:
NIST Quantum Cryptography Program Nears Completion
Huawei: Clear evidence of collusion' with Chinese Communist Party
Cellmate: Male chastity gadget hack could lock users in

In The News This Week

Software AG caught in double extortion ransomware hit

German software giant Software AG is racing to contain a major data leak resulting from a double extortion attack that saw its files encrypted and stolen by the operators of the Clop ransomware. The firm first came under attack on 3 October, and was forced to shut down its internal systems, forcing its helpdesk and internal communications offline, although its core customer-facing services, including its cloud-based services, were unaffected. At the time of writing, its online support system remained offline and customers were being asked to email a support address with details of their problem instead of using the standard interface. Clop's operators are understood to have demanded an exceptionally high ransom payment of $20m, but Software AG has refused to pay, so the gang has now begun to publish its confidential data on the dark web. Screenshots obtained by ZDNet show the leaked data to include scans of employees' identification, including passport details, internal emails and financial information. Such double extortion attacks are becoming increasingly common after first emerging about 12 months ago, because they give cyber criminals an additional means to apply pressure to their victims.
Read the full story here: ComputerWeekly

Hacker groups chain VPN and Windows bugs to attack US government networks

Some attacks were successful and intruders gained "unauthorized access to elections support systems." Hackers have gained access to government networks by combining VPN and Windows bugs, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) said in a joint security alert published on Friday. Attacks have targeted federal and state, local, tribal, and territorial (SLTT) government networks. Attacks against non-government networks have also been detected, the two agencies said. "CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised," the security alert reads. "Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks," officials also added. Attacks chained fortinet vpn and windows zerologon bugs . Read the full story by here: ZDNet Article

Treasury Dept. Advisory Shines Spotlight on Ransomware Negotiators

With attacks showing no signs of abating, some companies have begun offering services to help reduce ransom demands, buy more time, and arrange payments. The emerging ransomware negotiator industry has come into the spotlight recently following an advisory from the US Department of the Treasury for companies that facilitate ransom payments to threat actors on behalf of victims. The advisory, from the department's Office of Foreign Assets Control (OFAC), warned of potential regulatory trouble that such organizations could face if ransom payments ended up in the hands of adversaries on OFAC's Specially Designated Nationals and Blocked Persons List (SDN). US persons and entities are prohibited from conducting transactions with anyone on the SDN list or with any individual or organizations from countries that OFAC has officially sanctioned, such as North Korea, Iran, Ukraine, and Syria. Read the story by Jai Vijayan here: DarkReading

Twitter Locks Trump Campaign Account

Twitter temporarily suspended the account of the president of the United States' election campaign for "posting private information." The account @TeamTrump was locked for attempting to tweet a video referencing a recent article by the New York Post along with text describing presidential candidate Joe Biden as "a liar who has been ripping off our country for years." The New York Post article published leaked emails that suggest that in 2015, while working for Ukrainian natural gas firm Burisma Holdings, Biden's son Hunter arranged for the then Vice President Joe Biden to meet with a top executive at the company…
Read the story by Sarah Coble here: InfoSecurity

SIM swap fraud explained and how to help protect yourself

The topics of phone hacking, cloning and phone fraud headlined in many news articles and mobile phone forums in recent months and as we highlighted some of these topics in the last few bulletins, I thought it apt to carry on and explore some of the mechanism fraudsters use. SIM swap is one of these mechanisms and Alison Grace Johansen of Norton LifeLock wrote a good article on the subject last year which gave a good overview on the topic. Below then is an slightly adapted version of Alison's article.

Your cell phone could provide a way for cybercriminals to access your financial accounts. How? Through your mobile number. The fraud is known as SIM swapping, and it can be used to take over your financial accounts. SIM swapping relies on phone-based authentication. In a successful SIM swap scam, cybercriminals could hijack your cell phone number and use it to gain access to your sensitive personal data and accounts. Here's how it goes down. You might try to access one of your bank accounts that uses text-based two-factor authentication. That means you begin to access your account by entering your username and password. Your bank then sends an access code to your cell phone for you to complete the log-in process. But what if fraudsters are able to change the SIM card connected to your mobile number? That would give them control over that number — and they'd receive the access code to your account. It's a good idea to learn about of SIM card swapping. That way you can help protect yourself against this type of fraud — or recognize if you've become a victim. Here's what you need to know.

How do SIM swapping scams work? - A SIM swap scam (also known as SIM splitting, simjacking, sim hijacking, or port-out scamming) is a fraud that occurs when scammers take advantage of a weakness in two-factor authentication and verification in which the second step is a text message (SMS) or call to your mobile phone number. First, some SIM-card basics. Cell phone subscriber identity module (SIM) cards are the storage for user data in Global System for Mobile (GSM) phones. Without a SIM card, your GSM phone wouldn't be authorized to use a mobile network. So having control over your cell phone number would be valuable to fraudsters. To steal your number, scammers start by gathering as much personal information on you as they can get and engaging in a bit of social engineering. The scammers call your mobile carrier, impersonating you and claiming to have lost or damaged their (your) SIM card. They then ask the customer service representative to activate a new SIM card in the fraudster's possession. This ports your telephone number to the fraudster's device containing a different SIM. Or, they may claim that they need help switching to a new phone. How are fraudsters able to answer your security questions? That's where the data they've collected on you through phishing emails, malware, the dark web, or social media research becomes useful. Once they gain access to and control over your cell phone number, fraudsters can then access your phone communications with banks and other organizations, in particular, your text messages. They can then receive any codes or password resets sent to that phone via call or text for any of your accounts. And that's it: They're in.

How do they get your money? - They might set up a second bank account in your name at your bank — where, because you're already a bank customer, there may be less robust security checks. Transfers between those accounts in your name might not sound any alarms.

Social media and the SIM swap scam - Scammers can use your social media profiles to gather information on you that may help them impersonate you. For example, if your mother's maiden name or your high school mascot are answers to your security questions, a fraudster may be able to discover that information within your Facebook profile. But social media also can alert you to being victimized. Consider the high-profile example of a SIM swap scam against Twitter CEO Jack Dorsey. Dorsey's Twitter account was hacked when fraudsters gained control over his phone number — and went on to tweet offensive messages for the 15 minutes it took to regain control of his account.

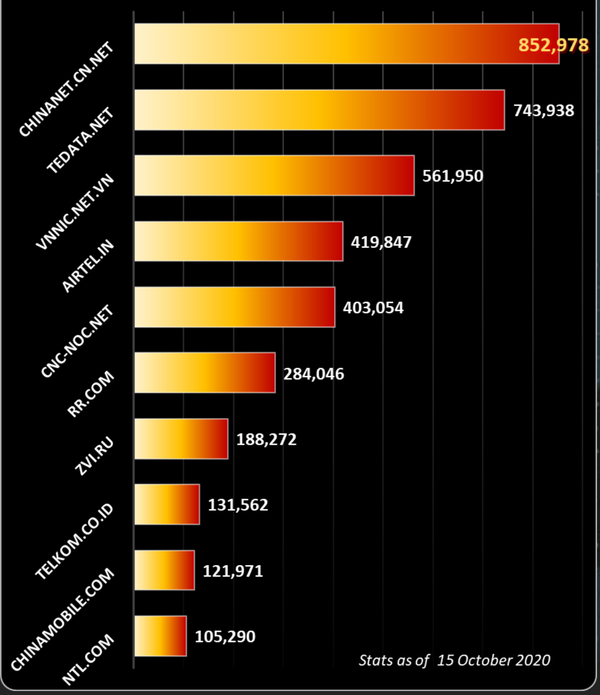
How did the hackers get access to his phone number? - They somehow convinced Dorsey's phone carrier to essentially swap SIM cards, assigning Dorsey's phone number to their SIM card and phone. They then used Cloudhopper's text-to-tweet service for Twitter.

Signs you may be a victim of SIM swap fraud - It can be challenging to stay ahead of SIM swap scams. It's important to recognize warning signs, so you can shut down the fraudsters' access as quickly as possible. One warning sign, as seen in Dorsey's case, is social media activity that isn't yours. The tweets made to Dorsey's Twitter account alerted him to the breach.

Here are three other signals you may be a victim of SIM swapping – **(1)** You're unable to place calls or texts. - The first big sign that you could be a victim of SIM swapping is when your phone calls and text messages aren't going through. This likely means fraudsters have deactivated your SIM and are using your phone number. (**2**) You're notified of activity elsewhere. - You'll know you're a victim if your phone provider notifies you that your SIM card or phone number has been activated on another device. **(3)** You're unable to access accounts. - If your login credentials no longer work for accounts like your bank and credit card accounts, you likely have been taken over. Contact your bank and other organizations immediately.

How can you protect yourself from SIM swap scams? – Due to space limitation I've extracted just a few points from Alison's article, please read the full article to see the all of the precautions you can take - • Online behaviour: - Beware of phishing emails and other ways attackers may try to access your personal data points extracted to help them convince your bank or cell phone carrier that they are you. • Account security: - Boost your cell phone's account security with a unique, strong password and strong questions-and-answers (Q&A) that only you know. • PIN codes - If your phone carrier allows you to set a separate passcode or PIN for your communications, consider doing it. It could provide an additional layer of protection. • Authentication apps: - You can use an authentication app such as Google Authenticator, which gives you two-factor authentication but ties to your physical device rather than your phone number.

Worst Botnet ISP's by number of Bots
Source https://www.spamhaus.org/statistics/botnet-isp/



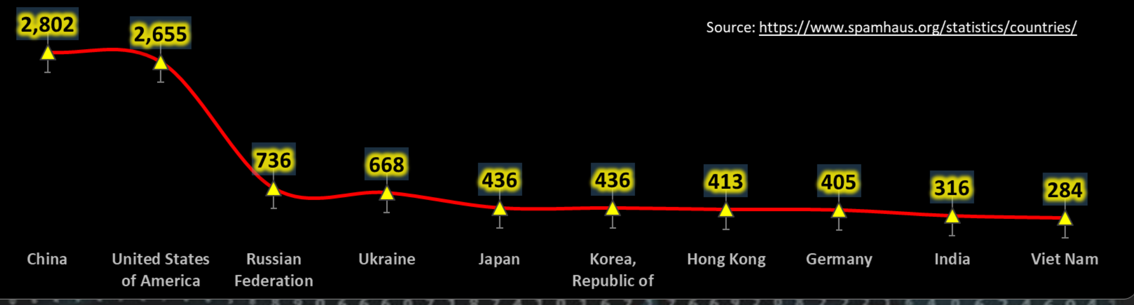
Stats as of 15 October 2020

For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

If you see an email from yourself to yourself, don't open it, it is most likely a spoof! Report it to your Cyber Security Team

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES) Data as on 16 October 2020

Source: https://www.spamhaus.org/statistics/countries/



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com