On May 4, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
06 May 22	515,898,572	6,272,172

Deaths this week: 15,596

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

06 May 2022

In The News This Week

Chinese "Override Panda" Hackers Resurface With New Espionage Attacks

A Chinese state-sponsored espionage group known as **Override Panda** has resurfaced in recent weeks with a new phishing attack with the goal of stealing sensitive information. "The Chinese APT used a spear-phishing email to deliver a beacon of a Red Team framework known as 'Viper,'" Cluster25 said in a report published last week. "The target of this attack is currently unknown but with high probability, given the previous history of the attack perpetrated by the group, it might be a government institution from a South Asian country. "Override Panda, also called Naikon, Hellsing, and Bronze Geneva, is known to operate on behalf of Chinese interests since at least 2005 to conduct intelligence-gathering operations targeting ASEAN countries.
Read the full story by Ravie Lakshmanan here: The Hacker News

New Raspberry Robin worm uses Windows Installer to drop malware

Red Canary intelligence analysts have discovered a new Windows malware with worm capabilities that spreads using external USB drives. This malware is linked to a cluster of malicious activity dubbed Raspberry Robin and was first observed in September 2021. Red Canary's Detection Engineering team detected the worm in multiple customers' networks, some in the technology and manufacturing sectors. Raspberry Robin spreads to new Windows systems when an infected USB drive containing a malicious .LNK file is connected. .
Read the article by Sergiu Gatlan here: Bleeping Computer

Bored Ape Thefts on Instagram Are Crypto's Latest Hack Headaches

When it comes to crypto hacks, the story is often the same: Scammers take advantage of a vulnerability in a blockchain's design and make off with millions, like in the $600 million-plus heist involving the play-to-earn NFT game Axie Infinity and the $77 million theft that took place Saturday on decentralized finance projects Rari Capital and Fei Protocol. But a $3 million hack last week involving nonfungible tokens from the popular Bored Ape Yacht Club universe exploited a different kind of weakness that isn't unique to blockchain. Scammers infiltrated the NFT collection's official Instagram account and posted a link to a fake website where users connected their crypto wallets for what they thought was an NFT launch. Read the rest of the story here: NDTV

Russia is losing the cyberwar against Ukraine, too

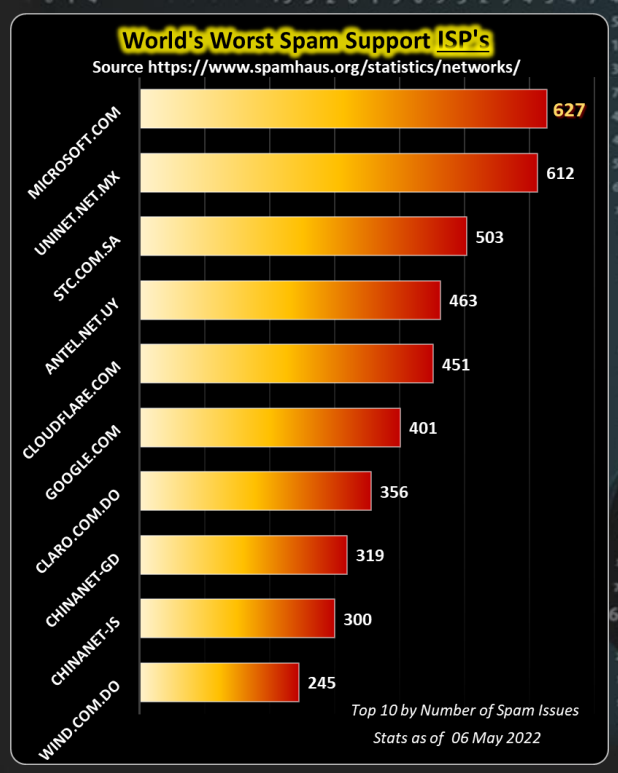
Not only has Russia seen setbacks on the battlefield in Ukraine, it's not faring well in the less obvious cyberwar either. One reason: Russia's ally Belarus was still using Windows XP to keep the trains running on time. When Russia launched its all-out attack against Ukraine in February, the world expected the invaders to roll over the country quickly. That didn't happen, and Ukraine today, though still under assault, has so far thwarted Russia's ambitions to conquer it. Russia has also been fighting a quieter war against Ukraine, a cyberwar, deploying what had been considered the most feared state-sponsored hackers in the world. And in the same way that Ukraine has fended off Russia's military might, it's been winning the cyberwar as well... Read the rest of the article by Preston Gralla here: Computerworld

Russian Hackers Targeting Diplomatic Entities in Europe, Americas, and Asia

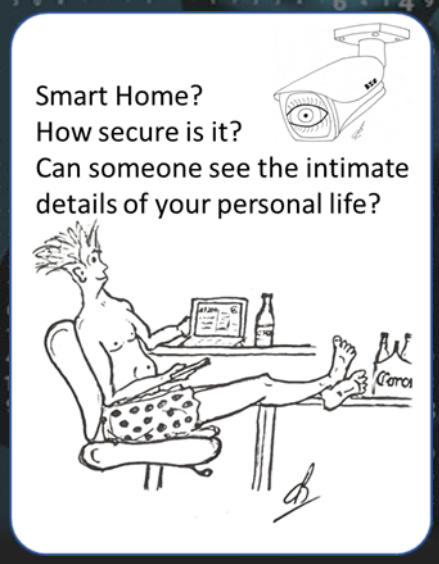
A Russian state-sponsored threat actor has been observed targeting diplomatic and government entities as part of a series of phishing campaigns commencing on January 17, 2022. Threat intelligence and incident response firm Mandiant attributed the attacks to a hacking group tracked as APT29 (aka Cozy Bear). "This latest wave of spear phishing showcases APT29's enduring interests in obtaining diplomatic and foreign policy information from governments around the world,".
Read the full article by Heather Ravi Lakshmanan here: The Hacker News

Anonymous Hackers Claim to Have Breached Russian Payment Service Provider Qiwi

Hackers from Network Battalion 65 (NB65), a group linked to the decentralized hacktivist collective Anonymous, revealed in a recent tweet they had hacked Qiwi, which is a major provider of payment and financial services in the Russian Federation and other countries in the post-Soviet space. A message posted by the @xxNB65 Twitter account notes that the group, which includes the Qiwi payment system, Qiwi Bank, the Contact money transfer system, and other platforms, also offers the most widely used payment app in Russia — that being the main reason why it was targeted.... "We will release 1 million records each day after your 3 day contract period has expired" the hackers have warned, adding that if there's someone to blame for the situation, that's Russian President Vladimir Putin.
Read the full article by Heather Lubomir Tassev here: Bitcoin



For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



Tips to Secure Your Smart Home and IoT Devices

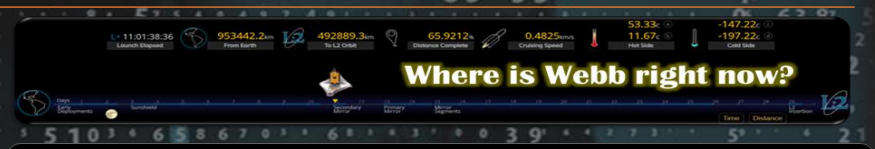
Last week we discussed how AI is stealthily encroaching on our daily lives. This week I want to extend the discussion into home automation and IoT devices, where the rapid expansion of AI technology can potentially open the door to either a carefree world or a security nightmare. Many media houses, over the last few years, has been reporting on IoT devices that were breached by hackers, like baby monitors, robotic vacuum cleaners, and so fourth, and intimate details of personal lives were exposed for all to see. Breaches happen from outside, but could your friendly AI vacuum cleaner perhaps pose a threat from the inside. That could be a bit far fetched, but for the moment, lets look at the threats Internet connectivity brings to your home and how you can secure it. Travis Goodreau of the IEEE Computer Society, wrote a good article with tips on how to secure your Smart Home and IoT devices. Following is an extract listing the main points of the article.

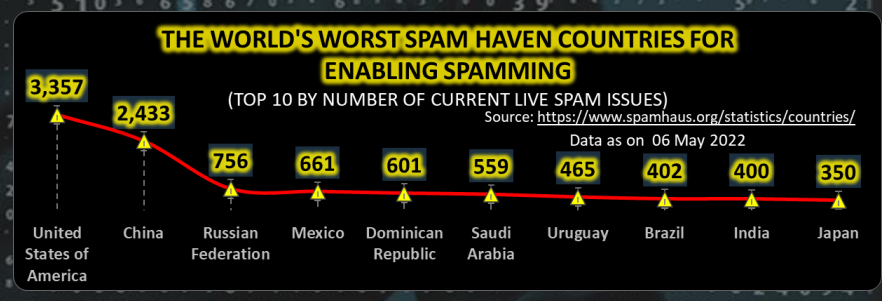
Tips to Secure Your Smart Home and IoT Devices

As you welcome the Internet of Things (IoT) into your home, turning it into a "smart" home, you're also likely making it an "insecure" home. Sure, a more connected home makes your life easier and more efficient. But with increased internet-based convenience comes an increased risk of becoming the target of cyberpunks. These hackers can steal and misuse your personal information and banking details, and even take control of those smart cameras or microphones to spy on you.
In other words, if you own smart devices such as smart speakers, TVs, thermostats, fridges, security cameras, and whatnot, your privacy and security could be at stake. Because, in essence, these are multiple entry points with rickety security that could leave you prone to attacks. So, long story short, if you're investing dough in setting up a smart home, you must also invest some time and energy in securing it. Here are a few ways to get started.
Set up Your Router Correctly (Lock the front door) - Your Wi-Fi router is the doorway to your smart home. You don't want it to break down in case a cybercriminal kicks it. And so, creating a more secure smart home starts with your router. It's what connects all your IoT devices and makes them so valuable. Follow these best practices to set up a secure router: (1) Change the Router's Default Name - Don't stick with your router's default name, which is usually its make and model. If people discover the make and model, they may be able to look up the default login and password and get easy access to your smart home network. So, change it to an unusual name that's not associated with you or your address. Be creative with your router name but don't give away any personal identifiers. (2) Set the Password to Something Unique - Similar to the router name, set the router's password to something truly unique. Use complex passwords made up of letters, numbers, and symbols. Consider using a random password generator to generate a near-impenetrable password. (3) Use the Highest Level of Encryption - Finally, go for the highest level of encryption, which currently is WPA2 or WPA3 if available. If your router only supports the WPA or WEP protocols, maybe it's time for an upgrade. Home routers are primary IoT targets for hackers. Thus, a secure router translates to a substantially more secure smart home.
Create a Separate Wi-Fi Network for IoT Devices - Many modern routers provide you the ability to set up a guest (or secondary) network. By creating a separate network dedicated to your IoT devices, you can safeguard your main network against IoT threats. This means relatives, friends, and guests can log into a network that isn't related to your IoT devices. So, your local smart home network is only accessible by you (and your family). As putting IoT devices on a different network keeps them detached, if hackers do manage to get through, they can't access any of your more important devices, such as your laptops or smartphones. Ofer Maor, a cybersecurity thought leader and board member of the OWASP Foundation says "I run my home on multiple network segments. There is my 'office' network with the laptops, NAS, and all the important sensitive parts of my home. There is my 'Home IoT' network, which holds most of the IoT devices. This limits a breach — if one of my IoT devices gets hacked, the hacker may be able to propagate from it to other IoT devices but will not be able to reach my laptop or my sensitive data."
Disable Features You Don't Use - Many IoT devices give you the ability to control them from anywhere on the planet. But if you only use them on your home's Wi-Fi connection, disable remote access. Likewise, smart speakers have Bluetooth connectivity in addition to Wi-Fi. Don't use it? Turn it off. Smart TVs come with voice control, but this feature often goes unused even in voice-controlled households where smart assistants such as Google Assistant, Siri or Alexa rule the roost. It may sound paranoid but an active mic, if hacked, can also be used to pry on your conversations. Thus, disabling features is all about blocking as many of those multiple entry points as possible.
Keep Your Devices Up-To-Date - Updates to your Wi-Fi router's firmware may not happen automatically. These updates often include essential security patches that can greatly enhance your network's security. So, see to it that you do a manual check every few months and if you find any pending firmware updates, install them right away. In the same vein, many IoT devices (and their apps) don't update automatically but prompt you to do so whenever available. Again, don't procrastinate; update straight away.
Enable Multi-Factor Authentication - Multi, typically two, -factor authentication (2FA) is an added layer of security beyond a mere password. With two-factor authentication, every time someone tries to log in to your IoT device, they have to provide additional proof of identity. This proof can come in the form of a one-time pin (OTP) or a verification code sent to your phone that confirms that the person logging in is indeed you. Most smart devices have the multi-factor authentication feature by default, but there are some devices that don't. In that case, you can enable 2FA by using third-party apps such as Google Authenticator.
Employ a Next-Generation Firewall (NGFW) - While your router has a built-in firewall, it may not prove to be sufficient. Because a traditional firewall lacks important security features like an intrusion prevention system (IPS), malware protection, content filtering, SSL/SSH interception, QoS management, and virtual private network (VPN). Next-generation firewalls are a fairly expensive investment, but the level of security boost for your smart home makes it a worthy investment. After all, if you can afford the devices, you can surely spend a little extra to secure them. By doing so, you're securing your privacy.
Please visit the IEEE Computer Society website for more tips and information.

Other Interesting News and Cyber Security bits:

- Rocket Lab catches rocket mid-air using helicopter before dropping it into the ocean
- Anonymous, anti-capitalist and awe-inspiring: were crop circles actually great art?
- SANS Daily Network Security Podcast (Storm cast)





AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com