On July 8, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Cisco, F5 and Google products.

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

10 July 2020

In The News This Week

North Korean Lazarus APT stole credit card data from US and EU stores

North Korea-linked hackers have been stealing payment card data from customers of large retailers in the U.S. and Europe for at least a year. Sansec researchers reported that North Korea-linked Lazarus APT group has been stealing payment card information from customers of large retailers in the U.S. and Europe for at least a year. The threat actors compromised legitimate websites to exfiltrate the stolen credit card data using an e-skimmer. In the past, the APT targeted banks and cryptocurrency exchanges, according to the experts the overall operations allowed the group to earn $2 billion. The activity of the Lazarus Group surged in 2014 and 2015, its members used mostly custom-tailored malware in their attacks and experts that investigated on the crew consider it highly sophisticated. The e-skimmer code used in the attacks shared the same codebase, the list of victims includes dozens of stores such as the accessories giant Claire's, Focus Camera, CBD Armour, Microbattery, and Realchems."
Read the full story here: Cyber defence

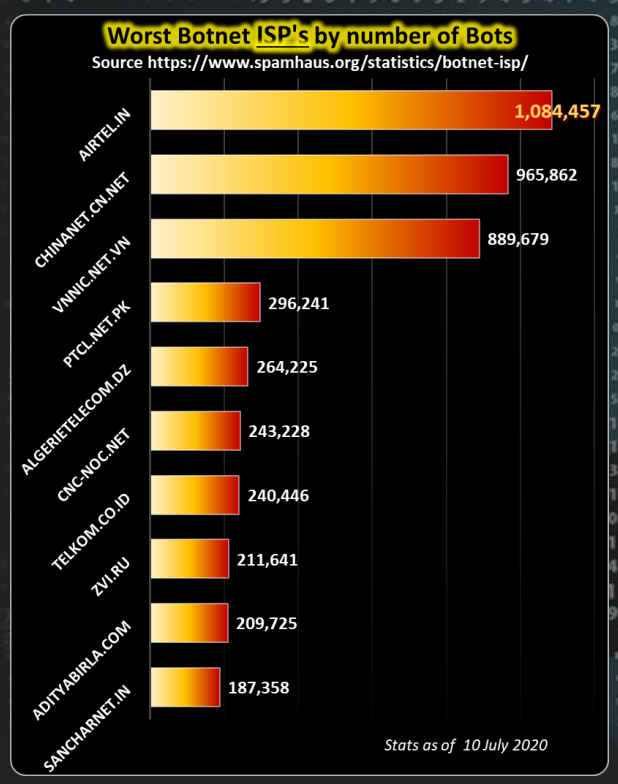
Hundreds arrested after encrypted messaging network takeover

European law enforcement agencies arrested hundreds of suspects in several countries including France, Netherlands, the UK, Norway, and Sweden after infiltrating the EncroChat encrypted mobile communication network used by organized crime groups. EncroChat phones used by international criminal networks around the world to exchange encrypted data and millions of messages came with dual operating systems (Android OS and the EncroChat OS). They also provided users with self-destruct messages, panic and password wipe, Secure Boot, tamper-proofing, and a brute force resistant FIPS 140-2 certified hardware cryptographic engine. EncroChat devices could also be remotely erased by the reseller or helpdesk on customer notice. EncroChat sold the cryptophones for roughly €1,000 each all over the world and customers could get six-month worldwide coverage subscriptions at a cost of €1,500 EUR with 24/7 support. According to the UK National Crime Agency (NCA), EncroChat had roughly 60,000 users worldwide with 10,000 of them active only in the UK. Read the full story here: BleepingComputer

Here we go again – more than two dozen Android apps caught stealing your data

Sketchy Android apps that spy on users and steal data have been a nagging presence inside Google's Play Store for a while now, despite the search giant's best efforts to rid its app marketplace of bad actors. Google pulled 25 malicious apps from the Google Play Store discovered by the French cybersecurity firm Evina. The apps could have stolen users' Facebook credentials as they racked up more than 2 million downloads. As much as Google keeps improving its proprietary app marketplace, sketchy app developers will never stop trying to sneak into the Google Play Store, evading the the company's defenses, to put its apps into the mix and awaiting your download. Which we saw yet another example of in recent days, with the revelation that Google has booted another batch of Android apps from the store, this time 25 apps caught in a position to steal users' Facebook login data. Evina, a French cybersecurity firm, disclosed this news in recent weeks, with its report that a single threat group developed the batch of apps that were made to look like everything from wallpaper and flashlight apps to mobile games. However, all the apps had the same goal, as Evina explains in its report of the fraud. "When an application is launched on your phone, the malware queries the application name," the company explains. "If it is a Facebook application, the malware will launch a browser that loads Facebook at the same time. The browser is displayed in the foreground which makes you think that the application launched it. When you enter your credentials into this browser, the malware executes javascript to retrieve them. The malware then sends your account information to a server. One thing to note is that when Google pulled the apps from the Play Store after Evina shared its findings, the search giant also disables the apps on the user's end — in addition to notifying the user via the Play Store's Play Protect service."
Read the full article here: BGR

(Thanks to my good friend and security specialist Yazan Shapsugh who pointed me to some of the news articles used)



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

Working from home? It is now up to you to keep your machine up to date to prevent perpetrators from exploiting unpatched vulnerabilities.

Want to become a Cyber Security Specialist?

In one of my previous bulletins I touched on the subject on how to become a white hat hacker with information on training courses available to achieve that. Today I want to extent into the broader spectrum on Cyber Security and options available to get you trained in the niche or generic areas of Cyber Security which also includes Governance, Risk and Compliance (GRC). Below then is some of the options you can explore.

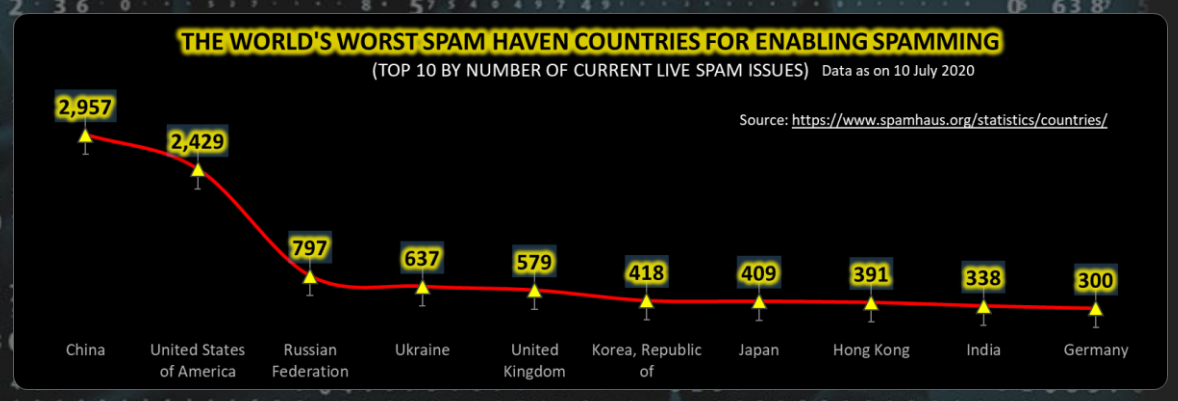
ISACA (Information Audit and Control Association) - ISACA offer a globally recognised certification covering the broader aspect of Information Security Management. The Certified Information Security Manager (CISM) certification indicates expertise in information security governance, program development and management, incident management and risk management. This is for those who want to take their career out of the technical realm into management, or those who are only interested in Security Management as a discipline. ISACA also offer certifications in IT Auditing (CISA) ,Risk Management (CRISC) and more. Please check out the ISACA website for full details.

SANS Institute – SANS is a well establish Information Security institution and is around since 1989. SANS offer a plethora of security courses, certifications and graduate programs including a Master of Science in Information Security Engineering. You can check out the full list of courses and certifications if you follow the highlighted link , following is a few examples:
Introduction to Cyber Security - This entry-level certification course covers a broad spectrum of security topics and is liberally sprinkled with real life examples. A balanced mix of technical and managerial issues makes this course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management. Security Essentials Bootcamp Style - This course is focused on providing you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems. Digital Forensics Essentials – This course provides the necessary knowledge to understand the Digital Forensics and Incident Response disciplines, how to be an effective and efficient Digital Forensics practitioner or Incident Responder, and how to effectively use digital evidence. Hacker Tools, Techniques, Exploits, and Incident Handling – This course will prepare you to turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. You will learn a time-tested, step-by-step process to respond to computer incidents. Smartphone Forensic Analysis In-Depth – This course is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, acquisition shortfalls, extraction techniques (jailbreaks and roots) and encryption.

(ISC)² Information Security Certification - (ISC)² is an international, non-profit membership association that offers a range of in-depth Cyber Security certifications including the coveted CISSP certification. CISSP – For the more technical minded, The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles. A word of caution though, this one is not for the faint hearted and I suggest that you build up to this one by following the Cyber Security Skills Roadmap set out by the SANS institute.

Now lets recap the certification route to become a White Hat or Ethical Hacker that I touched on previously - Many white hat hacking and security-related IT certifications can help a candidate get a foot in the door, even without copious amounts of hands-on experience. Achieving the Certified Ethical Hacker (CEH) certification from the EC-Council is one recommended starting point. The CEH is a vendor-neutral credential, and CEH-certified professionals are in high demand. The median salary of an ethical hacker is almost $80,000, according to PayScale, and the top range can climb to well over $100,000. On the consulting side, the EC-Council states that CEH professionals can expect to be paid $15,000 to $45,000 per contract or short-term assignment.
The intermediate-level CEH credential focuses on system hacking, enumeration, social engineering, SQL injection, Trojans, worms, viruses and other forms of attack, including denial of service (DoS). Candidates must also demonstrate thorough knowledge of cryptography, penetration testing, firewalls, honeypots and more. The EC-Council recommends a five-day CEH training class for candidates without prior work experience. To do well in the course, students should have Windows and Linux systems administration skills, familiarity with TCP/IP and working knowledge of virtualization platforms. However, self-study options are also available to help candidates pass the single required exam. Be aware that the EC-Council requires candidates to have at least two years of information security experience and to pay a $100 application fee. Becoming a certified white hat hacker also involves staying on the legal side of hacking, never engaging in illicit or unethical hacking activities and always protecting the intellectual property of others. As part of the certification process, candidates need to agree to uphold the EC-Council's code of ethics and never associate with unethical hackers or malicious activities.
In addition to the CEH, the SANS GIAC curriculum is worth a look. The organization has granted more than 81,000 credentials to date. Candidates who start with GIAC's Cyber Defense certs, beginning with the GSEC, might find themselves better positioned to climb through an active, well-respected and deep security curriculum. The GIAC Penetration Tester (GPEN) and the GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) are both noteworthy certs for aspiring white hat hackers.
Another set of ethical hacking certifications are offered by mile2. Mile2 also have a Cyber Security Certification Roadmap that you can explore.

I sincerely hope that the information provided will spark n interest in the field and set you off on a rewarding career in Cyber Security.



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