On November 15, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, Microsoft, and VMWare 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

22 November 2019

In The News This Week

Google Offering $1 Million to Hack Its Titan M Security Chip

Google has long used bug bounties to help it uncover security flaws in its products before they appear in attacks. It's also been among the most generous with the pay-outs for those bugs, but its latest revision of the Android Security Rewards Program is taking things to a whole new level. Security researchers who find a flaw in the company's Titan M security chip could net themselves as much as $1 million.

The Titan M security chip debuted in the Pixel 3 about a year ago, but it wasn't an entirely new design. Before the mobile Titan chip, Google designed a similar chip for its servers. In both cases, the use case is similar — Titan is a low-power microcontroller that cryptographically verifies important system components and keeps your most sensitive data separate from the main operating system.

The Titan M is a smaller version of the server chip that maintains the integrity of a Pixel phone's software. The idea of having a hardware-based secure element isn't new. ARM chips have a component called TrustZone that is separate from the main OS and Apple has a secure enclave on its A-series chips. Google's Titan M is a completely separate hardware component that isn't even connected to the SoC, theoretically offering even more security. Google has gone so far as to make the Titan M the key to your Google account, provided you configure 2-factor authentication to ping your phone. Read the full story here: ExtremeTech

Alert - Fake Flash software update notice tries to download malware onto your PC

Crooks have been hacking websites to deliver fake software update notices to more than 100,000 web users in an attempt to trick them into downloading malware that could take over their PCs.

The hacking campaign has two variations, according to tech security company Zscaler, which has been tracking it. In the first version, the crooks hack into insecure WordPress sites using the theme plugin vulnerability and inject malicious redirect scripts into the compromised site. This allows them to display a fake Flash Player update alert to the user over the compromised site, which aims to trick website visitors into starting a software update.

Once the user clicks the 'Update' button, the script downloads the malicious file. Even if the user clicks the 'Later' button, the redirect still occurs, taking the user to the same page to download the malicious file.

If installed, the Remote Access Trojan (RAT) malware will send the victim's information in an encrypted format to the attacker's site, allowing remote access to the victim's PC. Read the full story here: ZDNet Article

Rouen hospital turns to pen and paper after cyber-attack

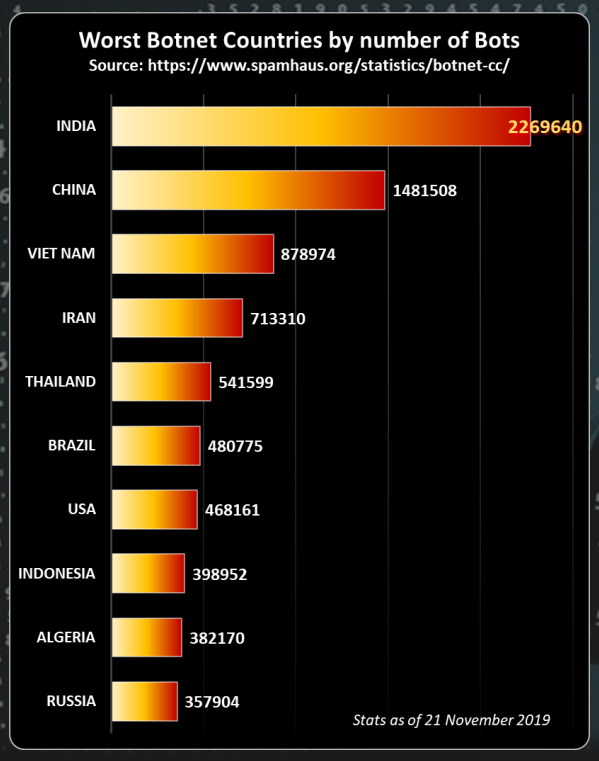
A cyber-attack on a hospital in Rouen last week caused "very long delays in care", reports the AFP news agency. Medical staff at the French city's University Hospital Centre (CHU) were forced to abandon PCs as ransomware had made them unusable, a spokesman said.

Instead, staff returned to the "old-fashioned method of paper and pencil", said head of communications Remi Heym. No patients were endangered as a result of the cyber-attack, the hospital said, in a statement published on Facebook.

The 1,300-bed hospital has not revealed details about the strain of ransomware with which it was infected. It said servers and many desktop PCs were rendered out of action by the attack, leaving staff to handle appointments by phone, issuing written prescriptions and reports. No medical or personal data has gone missing as a result of the attack, according to the hospital.

France's national cyber-crime agency, ANSSI, helped limit the scale of the outbreak, France's Le Monde newspaper reported. The paper reports that the agency also assisted with cleaning up computers infected by the virus, re-installing software and recovering encrypted files. The hospital stated it would not pay any ransom to have its files restored, adding that all its systems should be returned to normal by this weekend.

Read the full story here: BBC News Article



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

How to Become A White Hat Hacker

In my everyday conversations around cyber security, the topic of a career in cyber security often comes up and the youngsters always ask "but where do I start?". Below is an adapted and informative article by Ed Tittel and Earl Follis published in the Business News Daily that touches on this subject and offers some guidance to those who are curious enough about it.

What is a White Hat Hacker - A white hat hacker, or ethical hacker, uses penetration testing techniques to test an organization's IT security and identify vulnerabilities. IT security staff then uses the results of such penetration tests to remediate vulnerabilities, strengthen security and lower the organization's risk factors. Penetration testing is never a casual undertaking. It involves lots of planning, which includes getting explicit permission from management to perform tests, and then running tests as safely as possible. These tests often involve the very same techniques that attackers use to breach a network for real.

Background and education requirements

White hat hacking involves a great deal of problem-solving, as well as communication skills. A white hat hacker also requires a balance of intelligence and common sense, strong technical and organizational skills, impeccable judgment, and the ability to remain cool under pressure. At the same time, a white hat hacker needs to think like a black hat hacker, with all their nefarious goals and devious skills and behaviours. Some top-rate white hat hackers are former black hat hackers who got caught, and for various reasons, decided to leave a life of crime behind and put their skills to work in a positive (and legal) way. There are no standard education criteria for a white hat hacker – every organization can impose its own requirements on that position – but a bachelor's or master's degree in information security, computer science or even mathematics provides a strong foundation.

Pertinent certifications

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. Please check their Cyber Security Certification Roadmap.

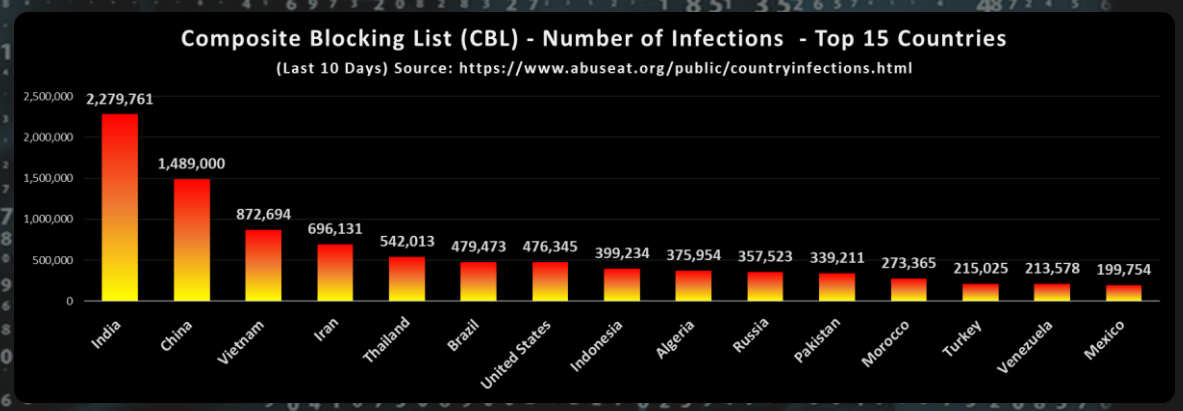
Related certifications in forensics

Some dabbling in computer forensics is always a good idea for somebody who works in information security. For those interested in the investigative side of security, continue with EC-Council's certification line-up and then tackle the Computer Hacking Forensic Investigator (CHFI) credential. The CHFI focuses on the forensics investigation process and utilizing the right tools and techniques to obtain computer forensic evidence and data. As part of the CHFI's certification training, candidates also learn how to recover deleted files, crack passwords, investigate network traffic and use a variety of forensic tools to gather information.

A few other worthy forensics-related certs include the GIAC Certified Forensics Analyst (GCFA) and the Certified Computer Forensic Technician and Certified Computer Crime Investigator certs from the High-Tech Crime Network.

The physical side of penetration testing

One more thing: Not all aspects of penetration testing are digital, nor do they always rely on digital means or methods of pursuit. Security experts generally refer to the security features of a site or facility, and physical access controls involved in entering or using facilities or equipment in person, under the heading of "physical security." Full-fledged penetration testing thus also involves attempts to compromise or circumvent physical security as well. Trained penetration testers may try to tailgate through an access gate, ask somebody to hold the door for them when seeking to bypass a badge reader or keypad entry control system, or use other forms of social engineering to get around physical security controls and barriers. Because getting up close and personal with equipment is a necessary first step in attacking its security, physical security and related security controls, policies and procedures are every bit as important as similar measures on the digital side of the security fence. Most information security certifications, including the CISSP, CISM, and Security+, provide some coverage of physical security in the common bodies of knowledge they ask candidates to learn and understand as they prepare for testing. - For those specifically interested in physical security, the Physical Security Professional (PSP) credential from ASIS International is probably the creme de la creme of physical security certifications. It's worth checking out for those who want to understand the full range of penetration testing methods, approaches and techniques, especially in the realm of physical security.



Author: Chris Bester
chris.bester@yahoo.com