The Cyber Threat Alert Level was evaluated on May 12 2021, and was set to Blue (Guarded), and will remain at this level until a change is indicated by CIS.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
09 July	186,330,643	4,026,186

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

09 July 2021

In The News This Week

Kaseya Attack - Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack

Hundreds of businesses around the world, including one of Sweden's largest grocery chains, grappled on Saturday with potential cybersecurity vulnerabilities after a software provider that provides services to more than 40,000 organizations, Kaseya, said it had been the victim of a "sophisticated cyberattack." Security researchers said the attack may have been carried out by REvil, a Russian cybercriminal group that the F.B.I. has said was behind the hacking of the world's largest meat processor, JBS, in May. In Sweden, the grocery retailer Coop was forced to close at least 800 stores on Saturday, according to Sebastian Elfors, a cybersecurity researcher for the security company Yubico. Outside Coop stores, signs turned customers away: "We have been hit by a large IT disturbance and our systems do not work." Mr. Elfors said a Swedish railway and a major pharmacy chain had also been affected by the Kaseya attack. "It's totally devastating," he said.." Read the full story by Kellen Browning here: NYT

Microsoft Releases Emergency Patch for PrintNightmare Bugs

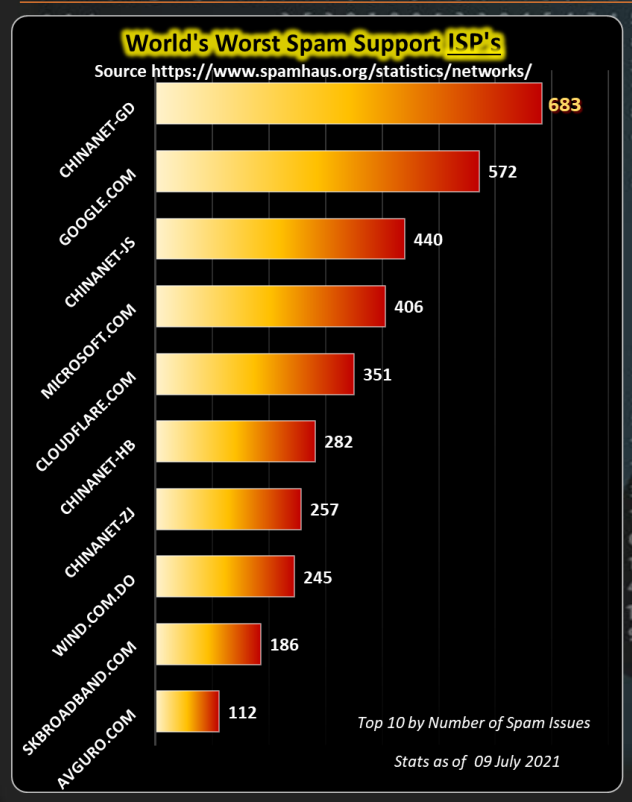
Microsoft has released an emergency patch for the PrintNightmare, a set of two critical remote code-execution (RCE) vulnerabilities in the Windows Print Spooler service that hackers can use to take over an infected system. However, more fixes are necessary before all Windows systems affected by the bug are completely protected, according to the federal government. Microsoft on Tuesday released an out-of-band update for several versions of Windows to address CVE-2021-34527, the second of two bugs that were initially thought to be one flaw and which have been dubbed PrintNightmare by security researchers. Read the full story here: ThreatPost

Cybercrime Costs Organizations Nearly $1.79 Million Per Minute

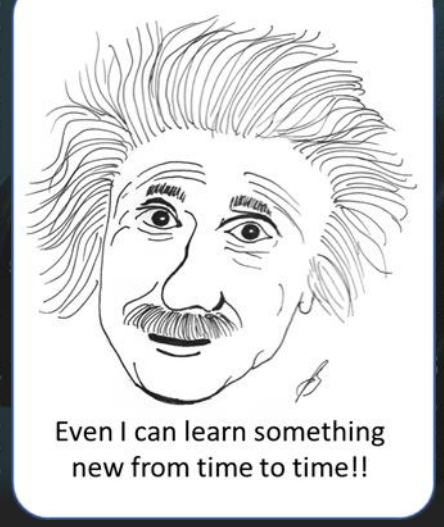
Cybercrime costs organizations an incredible $1.79m every minute, according to RiskIQ's 2021 Evil Internet Minute Report. The study, which analyzed the volume of malicious activity on the internet, laid bare the scale and damage of cyber-attacks in the past year, finding that 648 cyber-threats occurred every minute. The researchers calculated that the average cost of a breach is $7.2 per minute, while the overall predicted cybersecurity spend is $280,060 every minute. E-commerce has been heavily hit by online payment fraud in the past year, with cyber-criminals taking advantage of the shift to online shopping during the COVID-19 pandemic. While the e-commerce industry saw a record $861.1bn in sales, it lost $38,052 to online payment fraud every minute. Healthcare, another sector that has faced a surge in cyber-attacks since the start of COVID-19, lost $13 per minute on digital security breaches in the past year. The report also looked at the impact of different forms of cybercrime. It showed that per minute, there was $3615 lost to cryptocurrency scams, 525,600 records compromised and six organizations victimized by ransomware.. Read the full story by James Coker with more stats here: InfoSecurity Magazine

Hacker deposited $1M in a popular cybercrime marketplace to buy zero-day exploits

- A threat actor that goes online with the name "integra" has deposited 26.99 Bitcoins on one of the cybercrime forums with the intent to purchase zero-day Exploits from other forum members, researchers from threat intelligence firm Cyble. According to the experts, the member "integra" has joined the cybercrime forum in September 2012 and has gained a high reputation over the course of time. The threat actor is also a member of another cybercrime forum since October 2012. The threat actor aims at buying malware with zero detection,
The TA is willing to buy the following things with the deposited money zero-day exploits for RCE and LPE, in the latter case the member is offering up to $3 Million.
"The TA is willing to buy the following things with the deposited money." states Cyble.
(1) Buy the best Remote Access Trojan (RAT) that has not yet been flagged as malicious by any of the security products. **(2)** Buy unused start-up methods in Windows 10 such as living off the land (LotL) malware and hiding in the registry evasion technique. The TA is willing to offer up to USD 150K for the original solution. **(3)** Buy Zero Day Exploit for Remote Code Executions and Local Privileges Escalations. The TA has mentioned that the budget for this particular exploit is USD 3Million. Read the full story by Pierluigi Paganini here: Security Affairs



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



Weird Cyber Hacking Terms

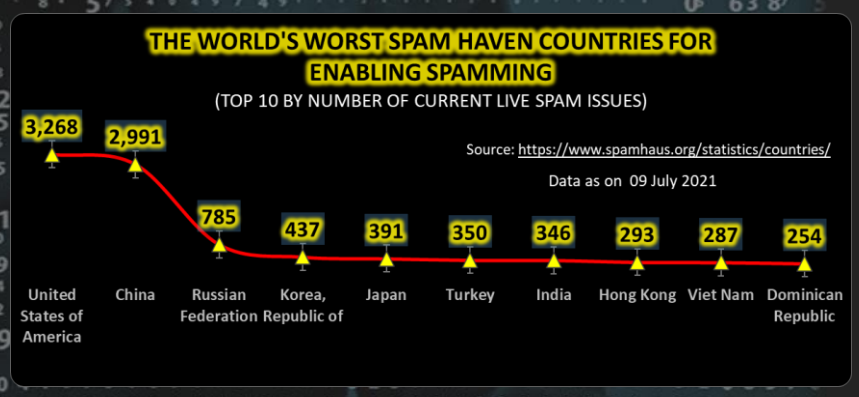
A couple of weeks ago, I said that I'll dedicate some time every once in a while to unpack and explain some of the cybersecurity jargon and terms you come across when you read about hacking. The guys at VICE came up with an e-Glossary of Cyber Terms and Hacking Lingo that I thought worthy of sharing. Below then is an extract of some of the not-so-common and weird ones.

- **Chip-off** - A chip-off attack requires the hacker to physically remove memory storage chips in a device so that information can be scraped from them using specialized software. This attack has been used by law enforcement to break into PGP-protected Blackberry phones.
- **Evil maid attack** - As the name probably suggests, an evil maid attack is a hack that requires physical access to a computer—the kind of access an evil maid might have while tidying his or her employer's office, for example. By having physical access, a hacker can install software to track your use and gain a doorway even to encrypted information.
- **Jailbreak** - Circumventing the security of a device, like an iPhone or a PlayStation, to remove a manufacturer's restrictions, generally with the goal to make it run software from non-official sources.
- **Lulz** - An internet-speak variation on "lol" (short for "laughing out loud") employed regularly among the black hat hacker set, typically to justify a hack or leak done at the expense of another person or entity. Sample use: y did i leak all contracts and employee info linked to Sketchy Company X? for teh lulz
- **Nonce** - A portmanteau of number and once, nonce literally means "a number only used once." It's a string of numbers generated by a system to identify a user for a one-time-use session or specific task. After that session, or a set period of time, the number isn't used again.
- **OTR** - What do you do if you want to have an encrypted conversation, but it needs to happen fast? OTR, or Off-the-Record, is a protocol for encrypting instant messages end-to-end. Unlike PGP, which is generally used for email and so each conversant has one public and one private key in their possession, OTR uses a single temporary key for every conversation, which makes it more secure if an attacker hacks into your computer and gets a hold of the keys. OTR is also generally easier to use than PGP.
- **Pwned** - Pwned is computer nerd jargon (or "leetspeak") for the verb "own." In the video game world, a player that beat another player can say that he pwned him. Among hackers, the term has a similar meaning, only instead of beating someone in a game, a hacker that has gained access to another user's computer can say that he pwned him. For example, the website "Have I Been Pwned?" will tell you if your online accounts have been compromised in the past.
- **RAT** - RAT stands for Remote Access Tool or Remote Access Trojan. RATs are really scary when used as malware. An attacker who successfully installs a RAT on your computer can gain full control of your machine. There is also a legitimate business in RATs for people who want to access their office computer from home, and so on. The worst part about RATs? Many malicious ones are available in the internet's underground for sale or even for free, so attackers can be pretty unskilled and still use this sophisticated tool.
- **Hashing** - Say you have a piece of text that should remain secret, like a password. You could store the text in a secret folder on your machine, but if anyone gained access to it you'd be in trouble. To keep the password a secret, you could also "hash" it with a program that executes a function resulting in garbled text representing the original information. This abstract representation is called a hash. Companies may store passwords or facial recognition data with hashes to improve their security.
- **Rainbow table** - A rainbow table is a complex technique that allows hackers to simplify the process of guessing what passwords hide behind a "hash" (see above).
- **Salting** - When protecting passwords or text, "hashing" (see above) is a fundamental process that turns the plaintext into garbled text. To make hashing even more effective, companies or individuals can add an extra series of random bytes, known as a "salt," to the password before the hashing process. This adds an extra layer of protection.
- **Tor** - Tor is short for The Onion Router. Originally developed by the United States Naval Research Laboratory, it's now used by bad guys (hackers, paedophiles) and good guys (activists, journalists) to anonymize their activities online. The basic idea is that there is a network of computers around the world—some operated by universities, some by individuals, some by the government—that will route your traffic in byzantine ways in order to disguise your true location. The Tor network is this collection of volunteer-run computers. The Tor Project is the non-profit that maintains the Tor software. The Tor browser is the free piece of software that lets you use Tor. Tor hidden services are websites that can only be accessed through Tor.
- **Tails** - Tails stands for The Amnesic Incognito Live System. If you're really, really serious about digital security, this is the operating system endorsed by Edward Snowden. Tails is an amnesic system, which means your computer remembers nothing; it's like a fresh machine every time you boot up. The software is free and open source. While it's well-regarded, security flaws have been found.
- **Warez** - Pronounced like the contraction for "where is" (where's), warez refers to pirated software that's typically distributed via technologies like BitTorrent and Usenet. Warez is sometimes laden with malware, taking advantage of people's desire for free software.

That's all we have space for today, please see the full glossary here: VICE

Other Interesting News and Cyber Security bits:

- How Fake Accounts and Sneaker-Bots Took Over the Internet
- NIST's Quantum Security Protocols Near the Finish Line.
- Branson vs Bezos vs Musk: Space tourism pioneers' reach for the stars



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