On September 1, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products.
See Latest CIS Advisories

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
03 Sep	219,958,506	4,557,117

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
03 September 2021

In The News This Week

Fired NY credit union employee nukes 21GB of data in revenge

Juliana Barile, the former employee of a New York credit union, pleaded guilty to accessing the financial institution's computer systems without authorization and destroying over 21 gigabytes of data in revenge after being fired. "In an act of revenge for being terminated, Barile surreptitiously accessed the computer system of her former employer, a New York Credit Union, and deleted mortgage loan applications and other sensitive information maintained on its file server," Acting U.S. Attorney Jacquelyn M. Kasulis said.
Over 20,000 documents destroyed within 40 minutes - According to court documents, the defendant worked remotely as a part-time employee for the credit union until May 19, 2021, when she was fired. Even though a credit union employee asked the bank's information technology support firm to disable Barile's remote access credentials, that access was not removed. Two days later, on May 21, Barile logged on for roughly 40 minutes.
Read the full story by Sergiu Gatlan here: BleepingComputer

WhatsApp issued second-largest GDPR fine of €225m

WhatsApp has been fined €225m (£193m) by Ireland's data watchdog for breaching privacy regulations. - It is the largest fine ever from the Irish Data Protection Commission, and the second-highest under EU GDPR rules. Facebook, which owns WhatsApp, has its EU headquarters in Ireland, and the Irish regulator is the lead authority for the tech giant in Europe. WhatsApp said it disagrees with the decision, and the severity of the fine, and plans to appeal. The fine relates to an investigation which began in 2018, about whether WhatsApp had been transparent enough about how it handles information. The issues involved were highly technical, including whether WhatsApp supplied enough information to users about how their data was processed and if its privacy policies were clear enough.. Read the full story here: BBC

FTC Bans SpyFone and CEO from Surveillance Business

FTC orders company to delete all secretly stolen data. - Today, the Federal Trade Commission banned SpyFone and its CEO Scott Zuckerman from the surveillance business over allegations that the stalkerware app company secretly harvested and shared data on people's physical movements, phone use, and online activities through a hidden device hack. The company's apps sold real-time access to their secret surveillance, allowing stalkers and domestic abusers to stealthily track the potential targets of their violence. SpyFone's lack of basic security also exposed device owners to hackers, identity thieves, and other cyber threats. In addition to imposing the surveillance-business ban, the FTC's order requires SpyFone to delete the illegally harvested information and notify device owners that the app had been secretly installed.
"SpyFone is a brazen brand name for a surveillance business that helped stalkers steal private information," said Samuel Levine, Acting Director of the FTC's Bureau of Consumer Protection. "The stalkerware was hidden from device owners, but was fully exposed to hackers who exploited the company's slipshod security. This case is an important reminder that surveillance-based businesses pose a significant threat to our safety and security. We will be aggressive about seeking surveillance bans when companies and their executives egregiously invade our privacy." Read the story by Scott Rosenberg here: FTC

New BrakTooth Flaws Leave Millions of Bluetooth-enabled Devices Vulnerable

A set of new security vulnerabilities has been disclosed in commercial Bluetooth stacks that could enable an adversary to execute arbitrary code and, worse, crash the devices via denial-of-service (DoS) attacks.
Collectively dubbed "BrakTooth" (referring to the Norwegian word "Brak" which translates to "crash"), the 16 security weaknesses span across 13 Bluetooth chipsets from 11 vendors such as Intel, Qualcomm, Zhuhai Jieli Technology, and Texas Instruments, covering an estimated 1,400 or more commercial products, including laptops, smartphones, programmable logic controllers, and IoT devices. The flaws were disclosed by researchers from the ASSET (Automated Systems SEcuriTy) Research Group at the Singapore University of Technology and Design (SUTD). "All the vulnerabilities can be triggered without any previous pairing or authentication," the researchers noted. ". Read the full story by Davey Winder here: The Hacker News

How ransomware runs the underground economy

Lucian Constantin of CSO wrote an interesting article this week on how the underground business of cybercriminals operates, and I thought it would be good to share an extract. Please read the full CSO article if this tickles your curiosity.

Ransomware gangs are adopting all the core elements of legitimate businesses—including defined staff roles, marketing plans, partner ecosystems, and even venture capital investments—and some hallmarks of more traditional criminal enterprises.
The unwanted attention attracted by ransomware attacks recently have caused several of the top cybercrime forums to ban ransomware discussions and transactions on their platforms earlier this year. While some hoped this might have a significant impact on the ability of ransomware groups to organize themselves, the bans only pushed their activity further underground, making it harder for security researchers and companies to monitor it.
If anything, the attacks in the months that followed the forum bans then have been more potent and audacious than ever. The truth is that ransomware is the life blood of the cybercrime economy and it will take extraordinary measures to put an end to it. The groups coordinating the attacks are highly professionalized and in many ways resemble modern corporate structures with development teams, sales and PR departments, external contractors and service providers that all get a cut from the illegal proceeds. They even use business lingo in their communications with victims, referring to them as clients who buy their data decryption services.
"The way I describe it is: You have the business world that we all know. The criminals have a parallel one that's like the Upside Down from Stranger Things. It's the exact same world, only darker and twisted," Steve Ragan, security researcher at Akamai, tells CSO.

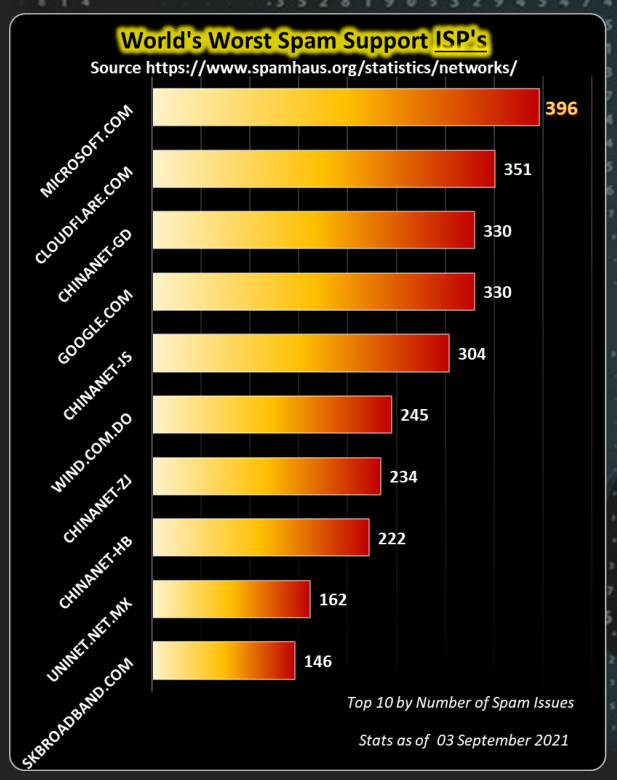
An underground economy relying on ransomware

By looking at what's involved in ransomware operations and how the groups are organized, it's easy to see that ransomware is at the center of the cybercrime economy. Ransomware groups employ people who: (1) Write file-encryption programs (the development team), (2) Set up and maintain the payment and leak sites, and the communication channels (the IT infrastructure team), (3) Advertise the ransomware service on forums (the sales team), (4) Communicate with journalists and post messages on Twitter and announcements on their blogs (the PR and social media team), (5) Negotiate the ransom payments (the customer support team), (6) Perform the manual hacking and lateral movement on victims' networks to deploy the ransomware program for a part of the profit (external contractors known as affiliates or penetration testers)
The affiliates often buy access into networks from other cybercriminals who already compromised systems with Trojan programs or botnets or through stolen credentials. These third parties are known as network access brokers. Affiliates might also buy data dumps that contain stolen account information or internal information that could help with target reconnaissance. Spam email services and bulletproof hosting are also often used by ransomware gangs.
In other words, a lot of parties are in the cybercrime ecosystem that directly or indirectly earn money thanks to ransomware. So, it's not unusual for these groups to become more professional and operate similar to companies with investors, managers, product marketing, customer support, job offerings, partnerships and so on. It's a trend that has been slowly building up over the years.
"The cybercrime underground has become essentially an economy unto itself where you have service providers, product creators, financiers, infrastructure providers," Brandon Hoffman, CISO of security firm Intel 471, tells CSO. "It's an economy just like ours where you have all these suppliers and buyers of different things. Just like in our free market economy, as you have all these different types of service providers and product providers available it's natural for them to start to come together and build a business together to offer a package of services and goods, just like we do here in the standard economy. So, I 100% agree that it is going that way. It's just really hard for us to prove it."
"We've known for years that criminals have a software development lifecycle just like the rest of us," Ragan says. "They have marketing, PR, middle management. They have people responsible for lower-level criminals who report to bigger-level criminals. It's not new. It's just that more people are starting to hear it and are paying attention to the parallels."

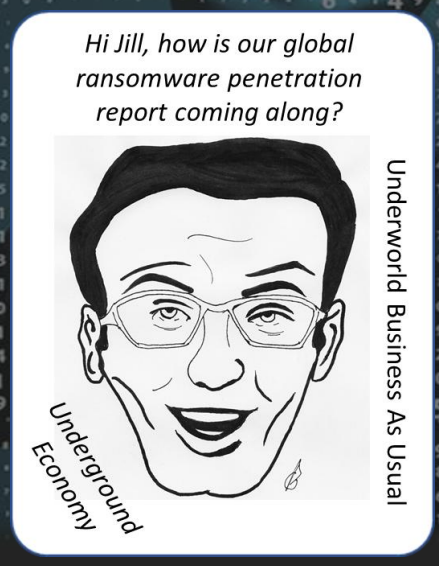
Ransomware groups adapt to market pressures

Ransomware attacks have crippled many hospitals, schools, public services, local and state government institutions and even police departments over the years, but the attack in early May on Colonial Pipeline, the largest pipeline system for refined oil products in the US, was a milestone.
The breach, attributed to a Russia-based ransomware group called DarkSide, forced the company to shut down its entire gasoline pipeline system for the first time in its 57-year history to prevent the ransomware from spreading to critical control systems. This resulted in fuel shortages across the US East Coast. The incident received widespread attention in the media and in Washington as it highlighted the threat that ransomware poses to critical infrastructure, spurring debates on whether such attacks should be classified as a form of terrorism.
Even the operators of DarkSide understood the seriousness of the situation and announced the introduction of "moderation" for its affiliates—the third-party contractors that actually do the hacking and deployment of the ransomware—claiming they want "to avoid social consequences in the future." But the heat was already too much for the group's service providers.
Only days after the attack, the administrator of XSS, one of the largest Russian-language cybercrime forums, announced the banning of all ransomware-related activities on the platform citing "too much PR" and heightening of law enforcement risks to "hazardous level," according to a translation by cybercrime intelligence firm Flashpoint.

That is all we have space for this week, please visit CSO to read the rest of the article.

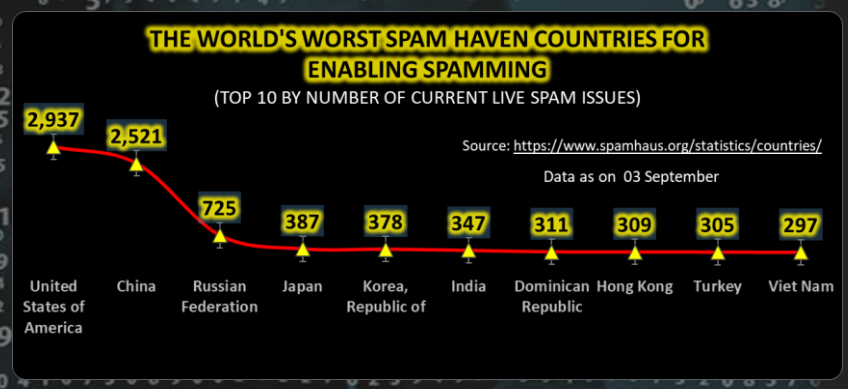


For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Other Interesting News and Cyber Security bits:

- Lightning cable look-alike for hackers now available for sale
- Windows 11 OVERVIEW
- Hacker sells tool for hiding malware inside graphics card VRAM



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