Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On April 7, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
09-Apr	134,548,721	2,915,432

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 April 2021

In The News This Week

Facebook data on 533 million users posted online

Data of 533 million Facebook users including phone numbers, Facebook IDs, full names, birth dates and other information have been posted online. The data dump was Tweeted by Alon Gal, CTO of security firm Hudson Rock. Gal posted a list of affected users by country. According to his list, the US had 32.3 million affected users and UK had 11.5 million. The data was accessed via a Telegram bot. Other data points in the posting included gender, location and job status. Catalin Cimpanu, at The Record, also reported that he reviewed samples of the leaked data and Facebook confirmed. The data is reportedly broken up into download packages by country. With the Facebook data out in the public it's safe to expect it to be used for cybercrime. Larry Dignan posted a couple of takeaway notes in the article which include this one: "The data is old" argument doesn't hold up. Facebook said the data was collected in 2019 and the company plugged the hole in August of that year. How often are phone numbers connected to Facebook changed? Not frequently if at all. Other information that was published includes full names and birth dates. It's unlikely that information changes either. It's also worth noting that two years old is pretty fresh in data time. Read the post by Larry Dignan here: ZDNet *(My friend Yazan Shapsugh pointed me to this story)*

Crime Service Gives Firms Another Reason to Purge Macros

Recent Trickbot campaigns and at least three common banking Trojans all attempt to infect systems using malicious macros in Microsoft Office documents created using EtterSilent. - A crime service gives attackers the ability to generate malicious Microsoft Word documents capable of compromising systems with hard-to-detect attacks, underscoring the continued danger posed by macros, according to a new analysis from threat intelligence firm Intel471. The service, known as EtterSilent, has rapidly become popular among cybercrime groups and allows attackers to create Word files that pose as DocuSign documents but, in reality, can compromise systems using either macros or by exploiting a known vulnerability. Windows systems configured to allow macros to be executed, or which have not been patched for the specific vulnerability, are at risk from files created by the service.
Read the full article by Robert Lemos here: Darkreading

Top cybercrime gangs use targeted fake job offers to deploy stealthy backdoor

The Golden Chickens cybercriminal gang is believed to sell its more_eggs backdoor for spear phishing campaigns executed using information gleaned from victims' LinkedIn profiles. - A group of criminals behind a stealthy backdoor known as more_eggs is targeting professionals with fake job offers tailored to them based on information from their LinkedIn profiles. The gang is selling access to systems infected with the backdoor to other sophisticated cybercrime groups including FIN6, Evilnum and Cobalt Group that are known to target organizations from various industries. Read the full article by Lucian Constantin here: CSO

States enact safe harbor laws against cyberattacks, but demand adoption of cybersecurity frameworks - Connecticut might soon follow Ohio and Utah by enacting a law that offers liability protection against ransomware and other cyberattacks, but only if victims follow security best practices. - While sophisticated ransomware and nation-state threat actors target US critical infrastructure, the only protection most organizations have against these attacks is tight and effective cybersecurity. These attacks have drawn government attention and sparked calls for liability protection against malicious intrusions. If organizations want this protection, however, lawmakers say they need to step up their game to implement better cybersecurity practices. During a Senate Intelligence Committee hearing last month, Chairman Mark Warner (D-VA) said, "While I am very open to some level of liability protection, I'm not interested in a liability protection that excuses the kind of sloppy behavior, for example, that took place in Equifax, where they didn't even do the basic cyber hygiene." "Cyber hygiene" is not enough, as former National Security Council (NSC) cybersecurity director Robert Knake recently wrote. "Basic cybersecurity hygiene, such as strong passwords, multifactor authentication, vulnerability patching, and next-generation antivirus software, is not sufficient against these groups," Knake wrote. "Instead, organizations should invest in security and operational vigilance, as these actors will take advantage of any mistake that defenders make." Read the story by Cynthia Brumfield here: CSO

Social Engineering

Social engineering is probably one of the most effective ways that cybercriminals are using to scam people or harvest personal information to either launch a sinister attack on the individual or his/her company. The motivation is almost always financial gain but political, social, or even revenge of some sort also comes into play. Wikipedia describes it as follows, "In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme."

Social Engineering is prying in on the emotional "pressure points" of people to invoke a response conducive to the perpetrator's sinister goal. Taking advantage of human emotion is much easier than hacking a network or looking for security vulnerabilities.

Here are some examples of how emotions can be exploited

Fear - You receive a voicemail that says you're under investigation for tax fraud and that you must call immediately to prevent arrest and criminal investigation. This social engineering attack happens during tax season when people are already stressed about their taxes. Cybercriminals prey on the stress and anxiety that comes with filing taxes and use these fear emotions to trick people into complying with the voicemail.

Greed - Imagine if you could simply transfer $10 to an investor and see this grow into $10,000 without any effort on your behalf? Cybercriminals use the basic human emotions of trust and greed to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information and the funds will be transferred the same day.

Curiosity - Cybercriminals pay attention to events capturing a lot of news coverage and then take advantage of human curiosity to trick social engineering victims into acting. For example, after the second Boeing MAX8 plane crash, cybercriminals sent emails with attachments that claimed to include leaked data about the crash. In reality, the attachment installed a version of the Hworm RAT on the victim's computer.

Helpfulness - Humans want to trust and help one another. After researching a company, cybercriminals target two or three employees in the company with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database – stressing that the manager needs it to make sure everyone gets paid on time. The email tone is urgent, tricking the victims into believing that they are helping out their manager by acting quickly.

Urgency – You receive an email from customer support at an online shopping website that you frequently buy from telling you that they need to confirm your credit card information to protect your account. The email language urges you to respond quickly to ensure that your credit card information isn't stolen by criminals. Without thinking twice and because you trust the online store, you send not only your credit card information but also your mailing address and phone number. A few days later, you receive a call from your credit card company telling you that your credit card has been stolen and used for thousands of dollars of fraudulent purchases.

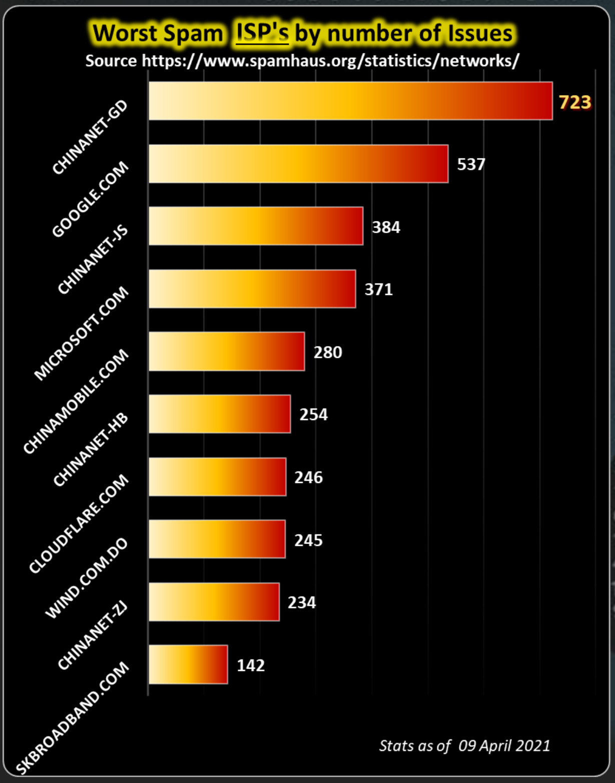
Some Real-life examples

Rimasauskas' $100 Million Scam – One of the biggest social engineering scams were perpetrated by Lithuanian national Evaldas Rimasauskas against two of the world's biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company's name. The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided, but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

Shark Tank - The host of the reality Television Show Shark Tank, Barbara Corcoran, lost close to $400,000 in an email scam when she thought she is corresponding with her assistant. Shark Tank showcases aspiring entrepreneurs from around the world where they pitch their business models to a panel of investors and persuade them to invest money in their idea.
Barbara Corcoran, a renowned real-estate broker revealed in February last year that she was scammed out of $380,000.
The scammers used an email address that looked like it belonged to Corcoran's assistant but was misspelled by one letter. Not picking up the misspelled address, Corcoran trusted the authenticity of the mail (which the scammers were bargaining on) that contained a fake invoice of a legitimate German renovations company that she was dealing with. It didn't raise any alarms as Corcoran invests in real estate. She authorised the payment of the invoice and the fraud was only picked up when the bookkeeper copied Corcoran's real assistant with the confirmation details. But by then it was too late. The scammers used social engineering techniques to get to know the most intricate details of Corcoran's life and business ventures. Like many business owners, Corcoran built a trust relationship with her assistant and had no reason to doubt the content of the mail, if only she picked up on the small spelling anomaly.

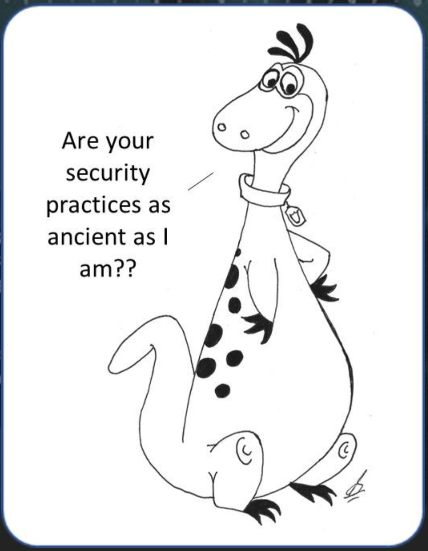
Cyber-assisted Deepfake Attack - In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring $243,000 to a "Hungarian supplier" — a bank account that actually belonged to a scammer.

References: Terranova, Forbes, Imperva, Tessian


Worst Spam ISP's by number of Issues
Source https://www.spamhaus.org/statistics/networks/

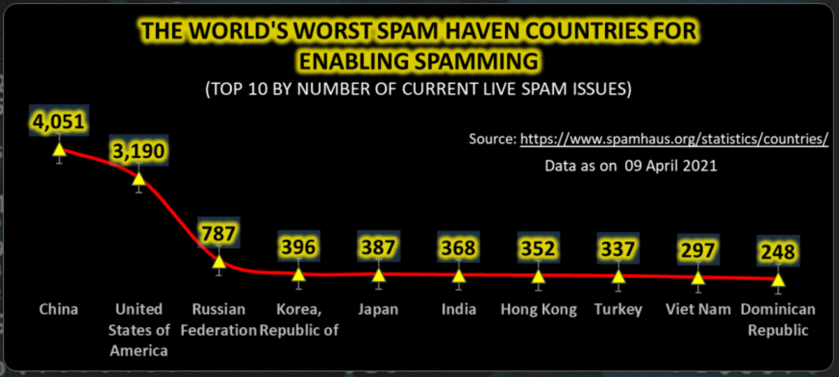
Stats as of 09 April 2021

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



Other Interesting News and Cyber Security bits:

- ❖ How shortages of a $1 chip sparked a crisis in the global economy
- ❖ This is where the iPhone hands down beats Android
- ❖ Did 4 Major Ransomware Groups Truly Form a Cartel?


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)
Source: https://www.spamhaus.org/statistics/countries/
Data as on 09 April 2021

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