On March 23, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
25 Mar 22	478,269,041	6,133,921

Deaths this week: 44,664

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
25 March 2022

In The News This Week

A Mysterious Satellite Hack Has Victims Far Beyond Ukraine

The biggest hack since Russia's war began knocked thousands of people offline. The spill over extends deep into Europe. – More than 22,000 miles above Earth, the KA-SAT is locked in orbit. Traveling at 7,000 miles per hour, in sync with the planet's rotation, the satellite beams high-speed internet down to people across Europe. Since 2011, it has helped homeowners, businesses, and militaries get online. However, as Russian troops moved into Ukraine during the early hours of February 24, satellite internet connections were disrupted. A mysterious cyberattack against the satellite's ground infrastructure—not the satellite itself—plunged tens of thousands of people into internet darkness.... Almost a month after the attack, the disruptions continue. Thousands still remain offline in Europe—around 2,000 wind turbines are still disconnected in Germany—and companies are racing to replace broken modems or fix connections with updates. Multiple intelligence agencies, including those in the US and Europe, are also investigating the attack. The Viasat hack is arguably the largest publicly known cyberattack to take place since Russia invaded Ukraine, and it stands out for its impact beyond Ukraine's borders. But questions about the details of the attack, its purpose, and who carried it out remain—although experts have their suspicions…
Read more from Matt Burgess here: Wired

Microsoft confirms they were hacked by Lapsus$ extortion group

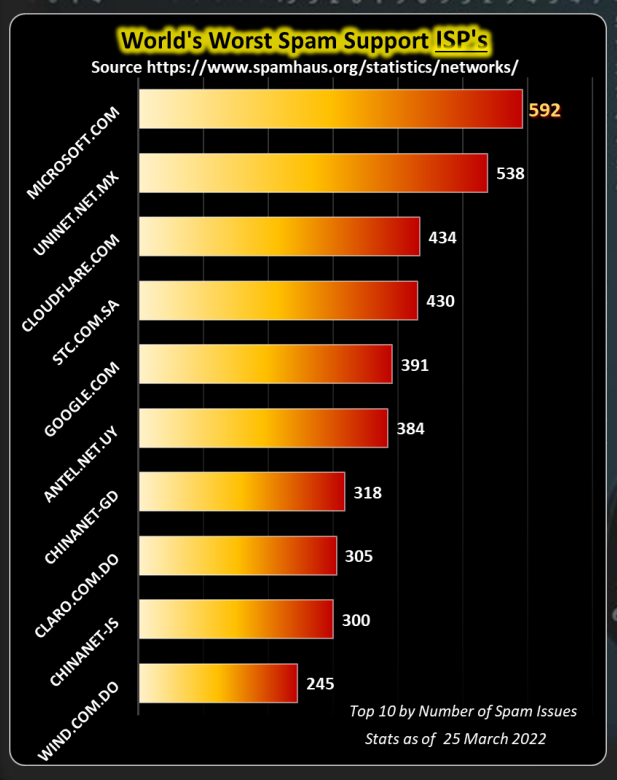
Microsoft has confirmed that one of their employees was compromised by the Lapsus$ hacking group, allowing the threat actors to access and steal portions of their source code. – On the evening of 21 March, the Lapsus$ gang released 37GB of source code stolen from Microsoft's Azure DevOps server. The source code is for various internal Microsoft projects, including for Bing, Cortana, and Bing Maps. In a new blog post published on 22 March, Microsoft has confirmed that one of their employee's accounts was compromised by Lapsus$, providing limited access to source code repositories. "No customer code or data was involved in the observed activities. Our investigation has found a single account had been compromised, granting limited access. Our cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity," explained Microsoft in an advisory about the Lapsus$ threat actors. "Microsoft does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk.
Read the rest of the story by Lawrence Abrams here: Bleeping Computer

Okta hack puts thousands of businesses on high alert

Okta, an authentication company used by thousands of organizations around the world, has now confirmed an attacker had access to one of its employees' laptops for five days in January 2022 and that around 2.5 percent of its customers may have been affected — but maintains its service "has not been breached and remains fully operational." The disclosure comes as hacking group Lapsus$ has posted screenshots to its Telegram channel claiming to be of Okta's internal systems, including one that appears to show Okta's Slack channels, and another with a Cloudflare interface. Any hack of Okta could have major ramifications for the companies, universities, and government agencies that depend upon Okta to authenticate user access to internal systems….
Read the rest of the story by Jon Porter and Sam Byford here: The Verge

Browser-in-the-Browser Attack Makes Phishing Nearly Invisible

Can we trust web browsers to protect us, even if they say "https?" Not with the novel **BitB** attack, which fakes popup SSO windows to phish away credentials for Google, Facebook and Microsoft, et al. - We've had it beaten into our brains: Before you go wily-nily clicking on a page, check the URL. First things first, the tried-and-usually-but-not-always-true advice goes, check that the site's URL shows "https," indicating that the site is secured with TLS/SSL encryption. If only it were that easy to avoid phishing sites. In reality, URL reliability hasn't been absolute for a long time, given things like homograph attacks that swap in similar-looking characters in order to create new, identical-looking but malicious URLs, as well as DNS hijacking, in which Domain Name System (DNS) queries are subverted. Now, there's one more way to trick targets into coughing up sensitive info, with a coding ruse that's invisible to the naked eye. The novel phishing technique, described last week by a penetration tester and security researcher who goes by the handle mr.d0x, is called a browser-in-the-browser (BitB) attack...
Read the rest of the article by Lisa Vaas here: ThreatPost



For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)

A closer look at phishing attacks

Phishing attacks are listed as the most prolific attack vector for hackers. Cybercriminals thrive on people's gullibility and general nature to respond to anything that has to do with, money or "urgent" messages, or things to do with health and beauty, and so on. We have seen it again this week, although not official, it is said that the Okta hack started with a phish. No matter how good your defenses are or how good your awareness campaign is, it only takes one click, and the stealthy underworld gears start turning. It sometimes amazes me how everyone is an expert on the subject in casual conversation, but still, they click. The Cisco Cybersecurity threat trends report claims that phishing accounts for almost 90% of all data breaches. That being said, as I was doing my usual foraging in the internet forest, I came across some must-know phishing statistics and insights by Maddie Rosenthal from Tessian that I would like to share today.

Must-Know Phishing Statistics – Updated 2022

Frequency of attacks - Phishing is a huge threat and growing more widespread every year. 2021 Tessian research found that employees receive an average of 14 malicious emails per year. Some industries were hit particularly hard, with retail workers receiving an average of 49. ESET's 2021 research found a 7.3% increase in email-based attacks between May and August 2021, the majority of which were part of phishing campaigns. And 2021 research from IBM confirmed this trend, citing a 2 percentage-point rise in phishing attacks between 2019 and 2020, partly driven by COVID-19 and supply chain uncertainty. CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations. The company's data suggests that phishing accounts for around 90% of data breaches. There's an uneven distribution in phishing attacks throughout the year. CISCO found that phishing tends to peak around holiday times, finding that phishing attacks soared by 52% in December. We've written about a similar phenomenon that typically occurs around Black Friday.

How phishing attacks are delivered - 96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone. When it's done over the telephone, we call it vishing and when it's done via text message, we call it smishing. The increase in phishing attacks means email communications networks are now riddled with cybercrime. Symantec research suggests that throughout 2020, 1 in every 4,200 emails was a phishing email. When it comes to targeted attacks, 65% of active groups relied on spear phishing as the primary infection vector. This is followed by watering hole websites (23%), trojanized software updates (5%), web server exploits (2%), and data storage devices (1%).

The most common subject lines - According to Symantec's 2019 Internet Security Threat Report (ISTR), the top five subject lines for business email compromise (BEC) attacks: (1) Urgent, (2) Request, (3) Important, (4) Payment and (5) Attention.

Analysis of real-world phishing emails revealed these to be the most common subject lines in Q4, 2020: (1) IT: Annual Asset Inventory, (2) Changes to your health benefits, (3) Twitter: Security alert: new or unusual Twitter login, (4) Amazon: Action Required - Your Amazon Prime Membership has been declined, (5) Zoom: Scheduled Meeting Error, (6) Google Pay: Payment sent, (7) Stimulus Cancellation Request Approved, (8) Microsoft 365: Action needed: update the address for your Xbox Game Pass for Console subscription, (9) RingCentral is coming!, (10) Workday: Reminder: Important Security Upgrade Required.

Link vs. attachment - Research from Cofense suggests phishing emails are slightly more like to contain a link to a malicious website (38%) than a malicious attachment (36%).

The most common malicious attachments - 2021 Tessian research suggests that **PDFs are the most common** type of malicious file attached with phishing emails. This trusted and versatile file format can be used to hide phishing links, run JavaScript, and deliver fraudulent invoices. SonicWall's 2021 Cyber Threat report suggests that there was a huge jump in the number of malicious PDFs and Microsoft Office files (sent via email) between 2018 and 2020. Workers are particularly likely to click these trusted formats. The volume of malicious Office and PDF files did start to dip in 2021, however, as some workers returned to working in the office. However, it's important to note—as users become more wary of opening suspicious-looking files—that many malicious emails don't contain an attachment. In fact, 2021 Tessian research found that 76% of malicious emails did not contain an attachment.

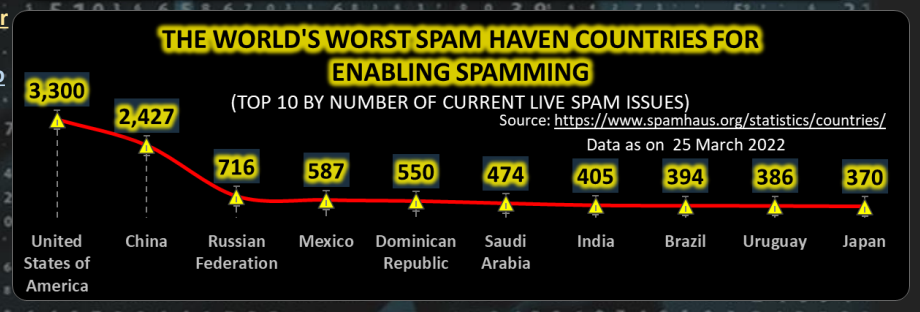
The data that's compromised in phishing attacks - The top three "types" of data that are compromised in a phishing attack are: (1) Credentials (passwords, usernames, pin numbers), (2) Personal data (name, address, email address), (3) Medical (treatment information, insurance claims)

The cost of a breach - In 2021, RiskIQ estimated that businesses worldwide lose $1,797,945 per minute due to cybercrime—and that the average breach costs a company $7.2 per minute. IBM's 2021 research into the cost of a data breach ranks the causes of data breaches according to the level of costs they impose on businesses. Phishing ranks as the second most expensive cause of data breaches—a breach caused by phishing costs businesses an average of $4.65 million, and Business Email Compromise (BEC) ranks at number one, costing businesses an average of $5.01 million per breach. That's not the only way phishing can lead to a costly breach—attacks using compromised credentials were ranked as the fifth most costly cause of a data breach (averaging $4.37 million). And how do credentials get compromised? More often than not, due to phishing.
According to Verizon, organizations also see a 5% drop in stock price in the 6 months following a breach. Losses from business email compromise (BEC) have skyrocketed over the last year. The FBI's Internet Crime Report shows that in 2020, BEC scammers made over $1.8 billion—far more than via any other type of cybercrime….

Unfortunately, that is all I have space for in this post, but please navigate to the Tessian page to read how Maddie Rosenthal unpack tons more stats and information for you.

Other Interesting News and Cyber Security bits:

- Microsoft help files repurposed to contain Vidar malware in new campaign
- What the heck happened to self-driving cars?
- Anonymous: Deadline up for companies still operating in Russia
- SANS Daily Network Security Podcast (Storm cast)



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