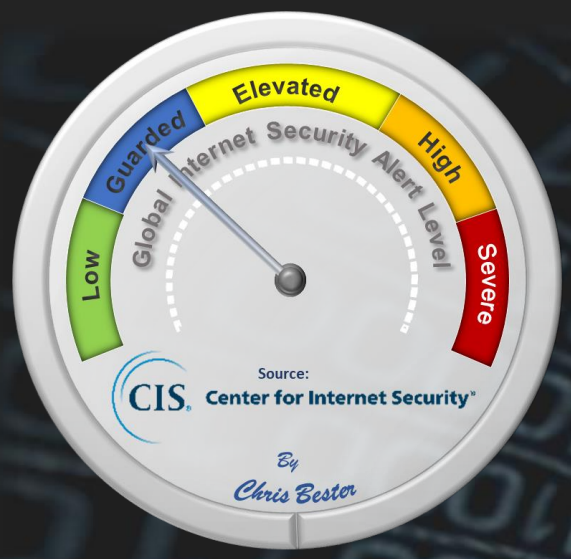


On December 10, the Cyber Threat Alert Level was evaluated and being raised to Blue (Guarded) due to vulnerabilities in Mozilla, Google, Apache, and Microsoft products.

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

11 December 2020

In The News This Week

Hackers are selling more than 85,000 MySQL databases on a dark web portal

Hackers break into databases, steal their content, hold it for ransom for 9 days, and then sell to the highest bidder if the DB owner doesn't want to pay the ransom demand. - More than 85,000 MySQL databases are currently on sale on a dark web portal for a price of only $550/database. The portal, brought to ZDNet's attention on Thursday by a security researcher, is part of a database ransom scheme that has been going on since the start of 2020. Hackers have been breaking into MySQL databases, downloading tables, deleting the originals, and leaving ransom notes behind, telling server owners to contact the attackers to get their data back. While initial ransom notes asked victims to contact the attackers via email, as the operation grew throughout the year, the attackers also automated their DB ransom scheme with the help of a web portal, first hosted online at sqldb.to and dbrestore.to, and then moved an Onion address, on the dark web. Victims who access the gang's sites are asked to enter a unique ID, found in the ransom note, before being presented with the page where their data is being sold. If victims don't pay within a nine-day period, their data is put up for auction on another section of the portal.
Read the full story by Catalin Cimpanu here: ZDNet Article

FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

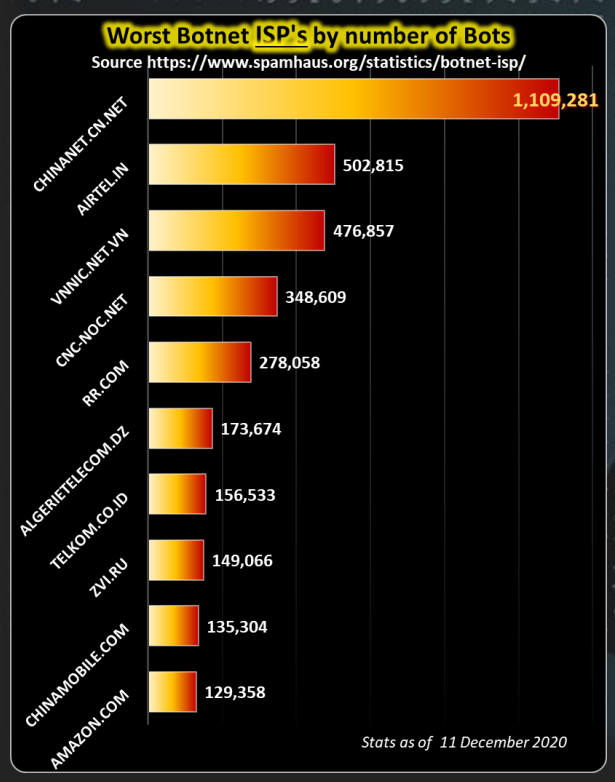
WASHINGTON — For years, the cybersecurity firm FireEye has been the first call for government agencies and companies around the world who have been hacked by the most sophisticated attackers, or fear they might be. Now it looks like the hackers — in this case, evidence points to Russia's intelligence agencies — may be exacting their revenge. FireEye revealed on Tuesday that its own systems were pierced by what it called "a nation with top-tier offensive capabilities." The company said hackers used "novel techniques" to make off with its own tool kit, which could be useful in mounting new attacks around the world. It was a stunning theft, akin to bank robbers who, having cleaned out local vaults, then turned around and stole the F.B.I.'s investigative tools. In fact, FireEye said on Tuesday, moments after the stock market closed, that it had called in the F.B.I. The $3.5 billion company, declined to say explicitly who was responsible. But its description, and the fact that the F.B.I. has turned the case over to its Russia specialists, left little doubt who the lead suspects were and that they were after what the company calls "Red Team tools." Read the full story here: NewYorkTimes *(Thanks to Yazan Shapsugh' input for this one)*

UK Ministry of Defence: We won't prosecute bug bounty hunters – oh btw, we now have one of those

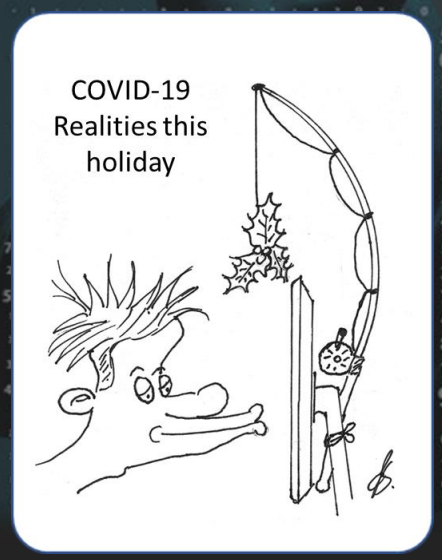
- The UK's Ministry of Defence has launched a bug bounty scheme, promising privateer pentesters they won't be prosecuted if they stick to the published script. The MoD has joined forces with bug bounty platform HackerOne, with the scheme seemingly being aimed at those who probe external web-facing parts of the ministry's sprawling digital estate. New guidance published on the GOV.UK pages for the MoD exhorts bug-hunters to submit only "benign, non-destructive, proof of concepts". "The MOD affirms that it will not seek prosecution of any security researcher who reports any security vulnerability on a MOD service or system, where the researcher has acted in good faith and in accordance with this disclosure policy," it stated.
Read the full story here: TheRegister

SABC confirms that its website was hacked

South Africa – The SABC has confirmed that its website was hacked and said it is working to resolve the issue. In response to queries sent by MyBroadband, acting SABC spokesperson Mmoni Seapolelo confirmed that the public broadcaster's TV Licence website had been compromised. "The SABC is aware of this matter and our Media and Technology Infrastructure department is attending to it," Seapolelo said. This follows after MyBroadband reported yesterday that the SABC TV Licence and SABC websites had been compromised and were redirecting users to phishing websites.
Read the full story here: MyBroadBand



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



Staying Safe on Social Networking Sites

Following on from last week's article on security resources offered by the National Cyber Security Alliance, the Cybersecurity & Infrastructure Security Agency (CISA) also offer a wealth of resources to help us stay safe. Today I want to share an adapted CISA article that talks about staying safe on social networking sites. Please visit the CISA page for the original article and other resources.

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections. Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messages) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest..

What security implications do these sites present?

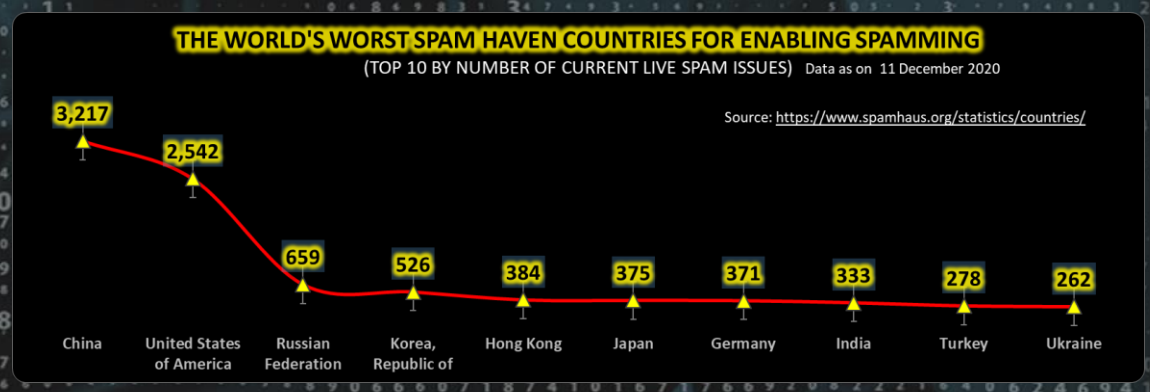
Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because: (a) the internet provides a sense of anonymity, (b) the lack of physical interaction provides a false sense of security, (c) they tailor the information for their friends to read, forgetting that others may see it, (d) they want to offer insights to impress potential friends or associates.

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available..

How can you protect yourself?

(1) Limit the amount of personal information you post - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections. (2) Remember that the internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines. (See Guidelines for Publishing Information Online.) (3) Be wary of strangers - The internet makes it easy for people to misrepresent their identities and motives. (See Using Instant Messaging and Chat Rooms Safely.) Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person. (4) Be skeptical - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action. (5) Evaluate your settings - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate. (6) Be wary of third-party applications - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access. (7) Use strong passwords - Protect your account with passwords that cannot easily be guessed. (See Choosing and Protecting Passwords.) If your password is compromised, someone else may be able to access your account and pretend to be you. (8) Check privacy policies - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. (See Reducing Spam.) Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join. (9) Keep software, particularly your web browser, up to date - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. (See Understanding Patches.) Many operating systems offer automatic updates. If this option is available, you should enable it. (10) Use and maintain anti-virus software - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. (See Understanding Anti-Virus Software.) Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

Please visit CISA for the full unabridged article and all the other the other amazing resources they offer.



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com