On November 12, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, Microsoft, and Google 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
13 November 2020

In The News This Week

2 More Google Chrome Zero-Days Under Active Exploitation

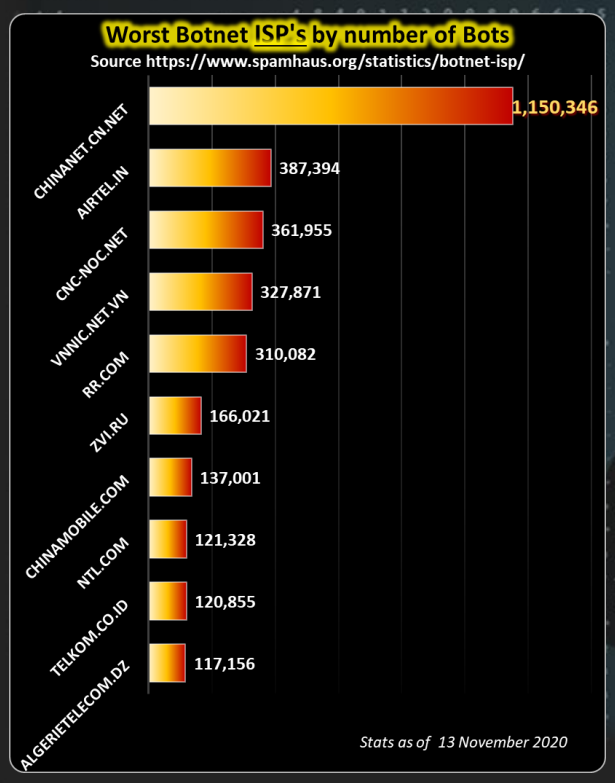
Google is asking Chrome desktop users to prepare to update their browsers once again as two more zero-day vulnerabilities have been identified in the software. Both allow an unauthenticated, remote attacker to compromise an affected system via the web. And both are being actively exploited in the wild, according to Google. The disclosure brings to five the total number of actively exploited flaws found in Chrome within the last three weeks. A stable channel update, 86.0.4240.198 for Windows, Mac and Linux, was released this week and will be rolled out "over the next days and weeks," Google Chrome's Prudhvikumar Bommana said in a blog post on Wednesday. The update will patch the two zero-day flaws, being tracked as CVE-2020-16013 and CVE-2020-16017. Both have a severity rating of "high," ranking 8.4 out of 10 on the CVSS bug-severity scale, and were reported by an anonymous source... Read the full story here: ThreatPost

Microsoft urges users to stop using phone-based text one-time-password and voice call multi-factor authentication

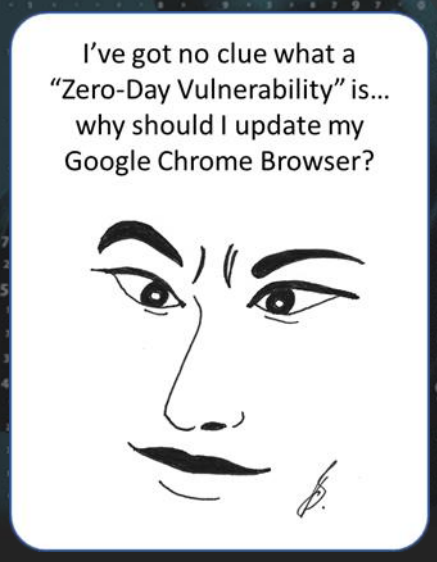
Microsoft is urging users to abandon telephone-based multi-factor authentication (MFA) solutions like one-time codes sent via SMS and voice calls and instead replace them with newer MFA technologies, like app-based authenticators and security keys. The warning comes from Alex Weinert, Director of Identity Security at Microsoft. For the past year, Weinert has been advocating on Microsoft's behalf, urging users to embrace and enable MFA for their online accounts. Citing internal Microsoft statistics, Weinert said in a blog post last year that users who enabled multi-factor authentication (MFA) ended up blocking around 99.9% of automated attacks against their Microsoft accounts. But in a follow-up blog post today, Weinert says that if users have to choose between multiple MFA solutions, they should stay away from telephone-based MFA. The Microsoft exec cites several known security issues, not with MFA, but with the state of the telephone networks today. Weinert says that both SMS and voice calls are transmitted in cleartext and can be easily intercepted by determined attackers, using techniques and tools like software-defined-radios, FEMTO cells, or SS7 intercept services. Weinert says that users should rather enable a stronger MFA mechanism for their accounts, if available, recommending off course, Microsoft's Authenticator MFA app as a good starting point. That does not mean that you should outright dismiss SMS and voice MFA, but if the option is available, rather use an App based authenticator. Read the full story by Duncan Riley here: ZDNet

Swiss report reveals new details on CIA spying operation

The CIA and German intelligence jeopardized Switzerland's historic reputation for neutrality by using a Swiss company as a platform for a global espionage operation for decades, according to a report released Tuesday by members of the Swiss parliament. Investigators concluded that Swiss authorities were aware of, and at times complicit in, an elaborate espionage operation in which the CIA covertly owned and controlled a Swiss company, Crypto AG, that secretly sold rigged encryption systems to foreign governments. The report marks the culmination of a Swiss investigation launched after the history of the Crypto operation was revealed earlier this year by The Washington Post in collaboration with ZDF, German public television, and Swiss broadcaster SRF. The Crypto operation exploited "Switzerland's image abroad as a neutral state," according to the report, which also said that Swiss authorities had effectively allowed the CIA and its German counterpart, the BND, to carry out "intelligence operations to the detriment of other states by hiding behind a Swiss company." The probe marks the first public accounting by a foreign government of an espionage operation so successful and extensive that a classified CIA history referred to it as "the intelligence coup of the century." The CIA did not respond to a request for comment, and the BND previously declined to comment. Crypto was one of the world's leading suppliers of encryption machines used by foreign governments. But the company was since the 1970s secretly owned by the CIA and the BND, and had clandestinely collaborated with the National Security Agency, the U.S. code-breaking service, beginning in the 1950s... Read the full story here: Washington Post



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



Zero-day vulnerability: What it is, and how it works

I'm sure all of you heard of the current spite of Zero-Day vulnerabilities in the mainstream media. A few people asked me this week, "What exactly is a Zero-Day vulnerability?" For corporates, this is one of the biggest fears as they are left bare bones until a solution is created and loaded on their respective environments. With the lucrative bug bounty programs, which most of the big software vendors started in recent years, more vulnerabilities are exposed than ever before. Below is a very high level overview by Norton.

Zero-day vulnerability: What it is, and how it works.

A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals.

What is a software vulnerability?

In the world of cyber security, vulnerabilities are unintended flaws found in software programs or operating systems. Vulnerabilities can be the result of improper computer or security configurations and programming errors. If left unaddressed, vulnerabilities create security holes that cybercriminals can exploit.

Why do vulnerabilities pose security risks?

Hackers write code to target a specific security weakness. They package it into malware called a zero-day exploit. The malicious software takes advantage of a vulnerability to compromise a computer system or cause an unintended behavior. In most cases, a patch from the software developer can fix this. What if your computer becomes infected? Exploit malware can steal your data, allowing hackers to take unauthorized control of your computer. Software can also be used in ways that were not originally intended — like installing other malware that can corrupt files or access your contact list to send spam messages from your account. It could also install spyware that steals sensitive information from your computer. If you're an everyday computer user, a vulnerability can pose serious security risks because exploit malware can infect a computer through otherwise harmless web browsing activities, such as viewing a website, opening a compromised message, or playing infected media.

What makes a vulnerability a zero-day?

The term "zero-day" refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released. So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers. Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users. But the software vendor may fail to release a patch before hackers manage to exploit the security hole. That's known as a zero-day attack.

What can you do to help protect yourself from zero-day vulnerabilities?

Zero-day vulnerabilities present serious security risks, leaving you susceptible to zero-day attacks, which can result in potential damage to your computer or personal data. To keep your computer and data safe, it's smart to take proactive and reactive security measures.

Your first line of defense is to be proactive by using comprehensive security software application that protects against both known and unknown threats.

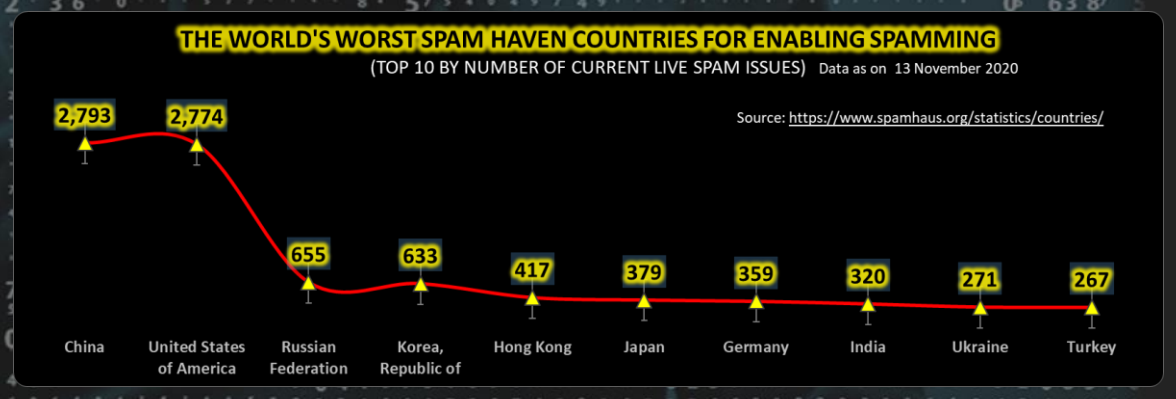
Your second line of defense is to be reactive and immediately install new software updates when they become available from the manufacturer to help reduce the risk of malware infection. Keep an eye on the news.

Software updates allow you to install necessary revisions to the software or operating system. These might include adding new features, removing outdated features, updating drivers, delivering bug fixes, and most important, fixing security holes that have been discovered.

Follow this security checklist to be sure you are doing everything you can to help keep your information protected from the security risks associated with zero-day vulnerabilities:

- Keep software and security patches up to date by downloading the latest software releases and updates. Installing security patches fixes bugs that the previous version may have missed.
- Establish safe and effective personal online security habits.
- Configure security settings for your operating system, internet browser, and security software.
- Install a proactive and comprehensive security software to help block known and unknown threats to vulnerabilities.

Read the full article by Norton's Kyle Chivers here: Norton Security



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