On July 15, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Juniper, SAP, Microsoft, Google, and Oracle 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
17 July 2020

In The News This Week

Massive Twitter Hack Infiltrated Multiple High-Profile Accounts Including Obama, Biden, Bezos - A major Twitter hack was perpetrated on Wednesday that resulted in multiple high-profile Twitter accounts being compromised. Among the hacked accounts were those of Apple, Elon Musk, and U.S. presidential candidate Joe Biden. All of the compromised accounts displayed similar messages that promised to double the amount of Bitcoin sent to a specific wallet address. The Bitcoin scam is a common one, but the fact that it was being broadcast from major verified Twitter accounts made it more likely that users would click on it. Also among the compromised accounts were those belonging to Kim Kardashian West, Jeff Bezos, Bill Gates, Barack Obama, Wiz Khalifa, Warren Buffett, and Michael Bloomberg. Multiple Twitter accounts belonging to others were compromised as well. While information is still coming out about the hack, what is known right now is that the perpetrator used internal Twitter admin tools to gain access to the accounts. Read the full story here: HotHardware

Critical flaw gives attackers control of vulnerable SAP business applications

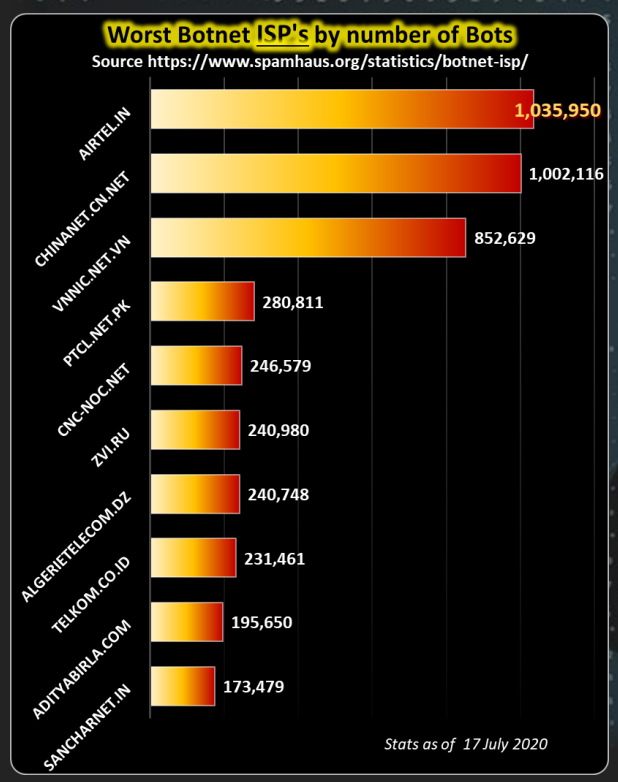
SAP has issued patches to fix a critical vulnerability (CVE-2020-6287) that can lead to total compromise of vulnerable SAP installations by a remote, unauthenticated attacker. The flaw affects a variety of SAP business solutions, including SAP Enterprise Resource Planning (ERP), SAP Supply Chain Management (SCM), SAP HR Portal, and others. Discovered and reported by Onapsis researchers and dubbed RECON, the CVE-2020-6287 vulnerability is due to the lack of authentication in a web component (LM Configuration Wizard) of the SAP NetWeaver AS for Java versions 7.30 to 7.50. The vulnerability can be exploited through an HTTP interface – typically exposed to end users and often to the internet. If successfully exploited, a remote, unauthenticated attacker can obtain unrestricted access to SAP systems through the creation of high-privileged users and the execution of arbitrary operating system commands with the privileges of the SAP service user account (adm), which is an unrestricted account.
Read the full article here: HelpNetSecurity

Ghost Squad Hackers defaced the European Space Agency (ESA) website

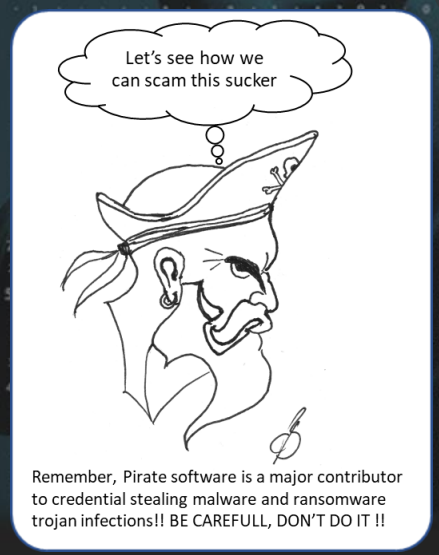
A group of hacktivists that goes online with the name Ghost Squad Hackers has defaced a site of the European Space Agency (ESA). Security Affairs have reached them for a comment and they told me that the attack was not targeted, they defaced the site only for fun. "We are hacktivists, we usually hack for many various causes related to activism." Ghost Squad Hacker's member s1ege told Security Affairs. "This attack was done solely for fun" The group claims to have hacked numerous organizations and government agencies over the years, including US military, European Union, Washington DC, Israeli Defense Forces, the Indian Government, and some central banks. The team appears to be focused primarily on operations against governmental agencies. When Security Affairs asked them for more details about the attack, the hackers explained that they have exploited a Server-side request forgery (SSRF) remote code execution vulnerability in the server, then they gained access to the business.esa.int domain and defaced it. A Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing.
Read more here: SecurityAffairs

Infosec inferno: Just 21% of security pros haven't considered quitting their current job

Almost one in five infosec pros have quit a job due to overwork or burnout caused by the constant pressure of keeping things safe and doing so without the resources to counter ever-evolving threats. This is the gloomy picture painted by a report from the Chartered Institute of Information Security (CIISec – previously known as IISP), which surveyed 445 security specialists. "In an era where workplace stress, mental illness, mindfulness and work-life balance are matters of importance and interest, we sought to understand if the security profession was at risk of burning itself out," the report, Security Profession 2019/2020 [PDF], stated. Read more here: TheRegister



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



Remember, Pirate software is a major contributor to credential stealing malware and ransomware trojan infections!! BE CAREFULL, DON'T DO IT !!

Pirate Software, dangers, effects and consequences

First, what is Software Piracy? Software piracy is the unauthorized copying or distribution of copyrighted software by duplicating, downloading, sharing, selling, or installing multiple copies onto personal or work computers. Using unlicensed software is illegal and increases security risks. Most countries with the exception of some countries in the far East have some form of legislation that criminalize software piracy. In the US for instance the federal copyright law denotes that "Users may not create a copy of a piece of software for any other reason other than as an archival backup without the permission of the copyright holder." What it comes down to, using, selling or distributing pirated software is stealing.

Panda Security states: "Software piracy has become a worldwide issue with China, the United States and India being the top three offenders. The commercial value of pirated software is $19 billion in North America and Western Europe and has reached $27.3 billion in the rest of the world. According to the 2018 Global Software Survey, 37% of software installed on personal computers is unlicensed software.
Software piracy doesn't require a hacker or skilled coder. Any normal person with a computer can become a software pirate if they don't know about the software laws. With such a widespread impact, it's important to understand what software piracy is and the dangers it presents."
Commercial losses suffered as a result of software piracy directly affect the profitability of the software industry. Because of the money lost to pirates, publishers have fewer resources to devote to research and development of new products, have less revenue to justify lowering software prices and are forced to pass these costs on to their customers.

Pirated software may have a cheaper price tag or could even be a free download, but be aware of the dangers and consequences of installing it such as:

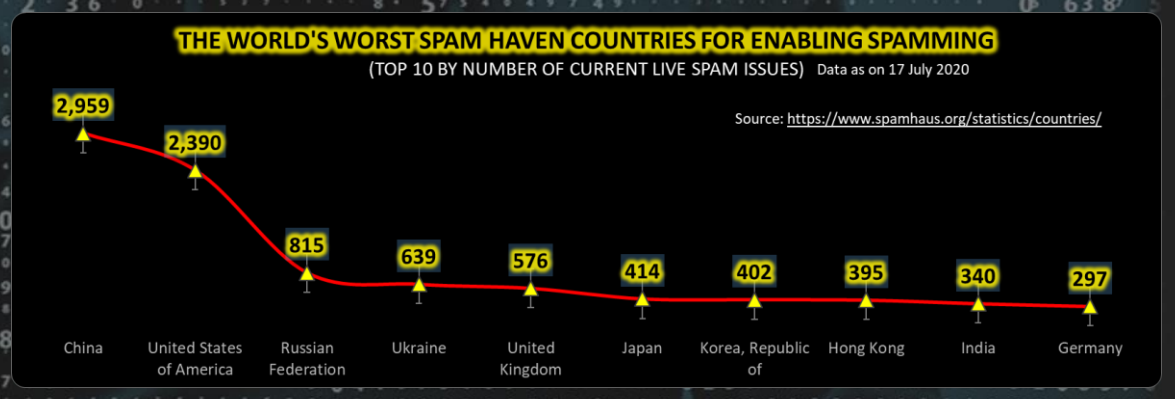
- Legal repercussions due to copyright infringement
- Increased risk of infecting your PC with malware, ransomware trojans, adware, etc.
- Increased chances of software malfunctions or failures
- Risk of adversely affecting your operating system causing "blue screen" or catastrophic hard drive failures.
- Forfeited access to support such as training, upgrades, helpdesk support and bug fixes
- No warranty and the pirated software can't be updated, you are stuck with the version you downloaded.
- Resource hogging that can slow down your PC
- Increased risk of infecting other PCs or Servers in your network if the software carries a malicious payload.

What can we do as Individuals to protect ourselves

- Always read the End User License Agreement, otherwise known as EULA, for each and every software program you purchase, the EULA states the terms and conditions that governs the usage of a specific software.
- The EULA will also outline the restrictions the vendor placed on the product which will include the number of copies you can make or machines you can install the the software on and also if you are permitted to create backup copies or not.
- For most software programs, you'll need to accept this agreement before you can install it. (I know most of us just click on "agree" without actually reading it, for all you know, you might be in breach of the copyright of the product, so take the time to read it)
- Ensure that you buy original software programs from certified re-sellers or from the original software vendor. Genuine software have authentication markings and/or seals. You can check the vendor's website to know what the original marking looks like.
- Using original software provide you with the ability to receive security updates or patches and upgrades when new versions are released.
- Note that when software is upgraded to a new version, it doesn't give a licensed user the right to copy, distribute, or sell the old version. An upgrade simply implies that the software has been improved. It ensures that the user continues to enjoy the reliability and quality assurance of the product.
- Do not download from Torrent or peer-to-peer websites and do not upload your software copies on these sites, in order to stop others from downloading your software copies, thereby implicating you in software piracy.
- Ensure that you register your software with the vendor.
- If you suspect that your software copy isn't authentic, or you suspect that a retailer or online seller is selling counterfeited copies, ensure to report them to the appropriate authorities. Doing this will go a long way in curbing software piracy. (See how you can report piracy below)

How and where can you report software piracy

- Report Piracy to the Federation Against Software Theft (FAST)
- Report Piracy to BSA The Software Alliance
- Report piracy to the Software and Information Industry Association (SIIA)
- Most of the major software vendors like Microsoft, Adobe, Oracle, etc. provide options to report piracy on their websites.



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