On September 15, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Google, Microsoft, and Adobe products.
See Latest CIS Advisories

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
17 Sep	227,760,798	4,681,533

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 September 2021

In The News This Week

BlackMatter Ransomware Hits Japanese Tech Giant Olympus

Japanese technology giant Olympus is currently investigating a cyber incident on its EMEA IT systems that happened earlier this month that sources said is the result of a BlackMatter ransomware attack. The company detected "suspicious activity" on Sept. 8 and "immediately mobilized a specialized response team including forensics experts," according to a press statement released over the weekend. "As part of the investigation, we have suspended data transfers in the affected systems and have informed the relevant external partners," according to the statement. "We are currently working to determine the extent of the issue and will continue to provide updates as new information becomes available."
Read the full story by Elizabeth Montalbano here: ThreatPost

HP Omen Hub Exposes Millions of Gamers to Cyberattack

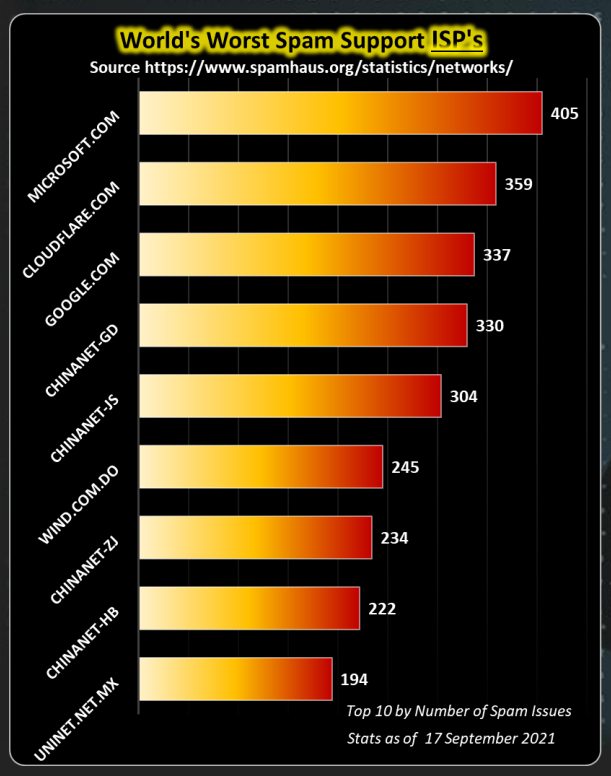
Millions of devices running the HP Omen Gaming Hub were using on a driver with a bug that could give attackers kernel-mode access without administrator privileges. HP has since released a patch, but a new report on the flaw (CVE-2021-3437) from researchers from SentinelLabs details how the gaming software was built in part by copying code from a problematic open-source driver called WinRing0.sys. HP Omen Gaming Hub is software that comes pre-installed on HP Omen desktops and laptops and functions as an optimizer for playing games, making automatic adjustments to fan speeds, lighting and accessory controls for the best gaming experience, SentinelLabs' report explained. Vulnerable HP OMEN Versions include: (1) HP OMEN Gaming Hub prior to version 11.6.3.0, (2) HP OMEN Gaming Hub SDK Package prior to version 1.0.44. Read the full story by Becky Bracken here: ThreatPost

You Can Now Sign-in to Your Microsoft Accounts Without a Password

Microsoft on Wednesday announced a new passwordless mechanism that allows users to access their accounts without a password by using Microsoft Authenticator, Windows Hello, a security key, or a verification code sent via SMS or email. The change is expected to be rolled out in the coming weeks.
"Except for auto-generated passwords that are nearly impossible to remember, we largely create our own passwords," said Vasu Jakkal, Microsoft's corporate vice president for Security, Compliance, and Identity. "But, given the vulnerability of passwords, requirements for them have gotten increasingly complex in recent years, including multiple symbols, numbers, case sensitivity, and disallowing previous passwords."
"Passwords are incredibly inconvenient to create, remember, and manage across all the accounts in our lives," Jakkal added. Over the years, weak passwords have emerged as the entry point for a vast majority of attacks across enterprise and consumer accounts, so much so that Microsoft said there are about 579 password attacks every second, translating to a whopping 18 billion every year. Read Ravie Lakshmanan's story here: The Hacker News

3 Former U.S. Intelligence Officers Admit to Hacking for UAE Company

The U.S. Department of Justice (DoJ) on Tuesday disclosed it fined three intelligence community and military personnel $1.68 million in penalties for their role as cyber-mercenaries working on behalf of a U.A.E.-based cybersecurity company. The trio in question — Marc Baier, 49, Ryan Adams, 34, and Daniel Gericke, 40 — are accused of "knowingly and wilfully combine, conspire, confederate, and agree with each other to commit offenses, "furnishing defense services to persons and entities in the country over a three year period beginning around December 2015 and continuing through November 2019, including developing invasive spyware capable of breaking into mobile devices without any action by the targets.
"The defendants worked as senior managers at a United Arab Emirates (U.A.E.)-based company (U.A.E. CO) that supported and carried out computer network exploitation (CNE) operations (i.e., 'hacking') for the benefit of the U.A.E. government," the DoJ said in a statement. "Despite being informed on several occasions that their work for [the] U.A.E. CO, under the International Traffic in Arms Regulations (ITAR), constituted a 'defense service' requiring a license from the State Department's Directorate of Defense Trade Controls (DDTC), the defendants proceeded to provide such services without a license."
Click on the links to read the US DoJ statement & Hacker News Article



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

Free tools to enhance the security on your personal PC

Let's be honest, we all like free stuff, but if it comes to cybersecurity, free stuff that you download can be loaded with other stuff like malware and spyware and so on. The good news is that some cyber security companies offer free tools to help you maintain a good security posture. It is kind of an oxymoron, free stuff to help you be safe from other free stuff. Fortunately, these tools are not just to manage our bad downloading habits but will help you to keep a fairly decent security posture on your personal computer. You must bear in mind, however, that free tools are not necessarily a substitute for tried and test subscription-based security offerings as there is no warranty or obligation to you from the provider. My aim today is not to downplay any good subscription-based security solution but to enhance that what you have. So, if you don't have anything, this is a good place to start, and if you are a subscriber or user of paid-for offerings, these tools will help to enhance your security posture. The selected items below are from a list compiled by Heimdal Security, please visit the site to see a full list.

The Free Security Tools & Software You Can Use for Your Online Protection

Data Breach Checking Tools

1. IDENTITY THEFT CHECKER - Powered by f-secure this is a tool specially designed to check whether your private information appears in data breaches. The email address or breach information won't be stored, making this tool completely safe to use. It works instantly, you just type your email address in, and the tool checks if any personal information that was tied to the email address provided was exposed in data breaches.
2. BREACH ALARM - If you think that your password might've been breached at any given time you can actually check this with the use of Breach Alarm, a tool that allows you to check anonymously if your password has been posted online, and sign up for email notifications about future password hacks that might affect you.
3. HAVE I BEEN PWNED? - Have I been pwned is another important tool that you can use as it has access to a large database of passwords when cross-referencing yours in order to show you if your password was involved in a data breach.

Tools to Scan URL's & Website Security

1. VIRUS TOTAL - VirusTotal works by inspecting items by using over 70 antivirus scanners and URL/domain block listing services. The users are able to select a file from their computer and send it to VirusTotal just by using their browser. VirusTotal offers a number of file submission methods, including the primary public web interface, desktop uploaders, browser extensions, and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.
2. SUCURI - SUCURI is one of the most popular free website malware and security scanner that can help you quickly test for malware, blacklisting status, injected SPAM, and defacements.
3. SITEGUARDING - SiteGuarding scans your domain for malware, website blacklisting, injected spam, defacement, and other possible threats, and is compatible with WordPress, Joomla, Drupal, Magento, osCommerce, and Bulletin.

Free Antivirus Software

1. MICROSOFT DEFENDER - The free Microsoft Defender Antivirus software running on Windows 10, offers you a malware protection safety net as the free antivirus program is built into Windows 10 and it's turned on by default. Fortunately, this free antivirus solution will cover the basics of internet security. You should note that Windows 10 will automatically disable its own Windows Defender antivirus if you install a third-party antivirus.
2. CLAMAV - ClamAV® is an open-source (GPL) anti-virus engine used in a variety of situations including email scanning, web scanning, and endpoint security. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command-line scanner, and an advanced tool for automatic database updates.
3. IMMUNET - Immunet is a free, cloud-based, community-driven antivirus application, using the ClamAV and its own engine. The software is complementary to existing antivirus software. In January 2011 Immunet was acquired by Sourcefire. The application is free of charge, although a commercial version is available.
4. COMODO - Comodo Internet Security is developed and distributed by Comodo Group, a freemium Internet security suite that includes an antivirus program, personal firewall, sandbox, host-based intrusion prevention system, and website filtering.

Software Updaters

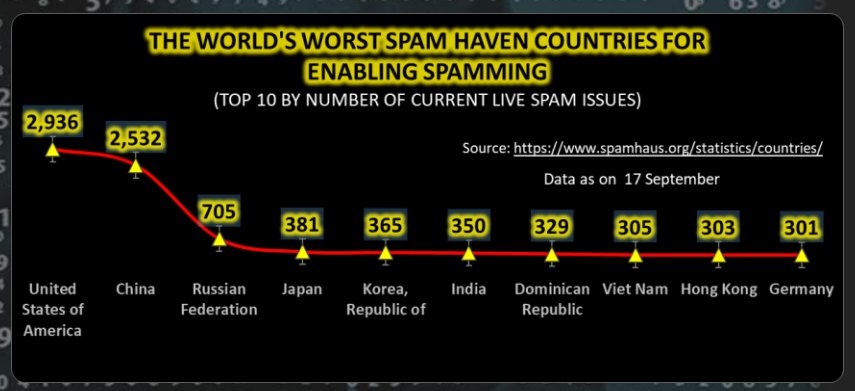
1. HEIMDAL™ FREE - This is a software updater for Windows PCs. It works by automating any software updates and in this way improving your security. Heimdal™ Free keeps your vulnerable applications up to date automatically and eliminates vulnerabilities used in cyber-attacks.
2. DOWNLOADCREW UPDATESCANNER - This candidate has access to one of the largest software databases on its market. The updater remains active in the background and in your system tray – will alert you when a priority update is ready.
3. PATCH MY PC HOME UPDATER - Patch My PC Home Updater is one of the more popular and most trusted software updaters in the free zone of these applications. Once installed it will scan your program library as soon as the program is initiated. Once this process is completed it will let you know without any further delays the important programs that have updates pending. With one mouse click, you can set all or some of those updates into motion.

PC Cleaners & Optimizers

1. ADVANCED SYSTEMCARE - Advanced SystemCare focuses on cleaning, optimizing, speeding up, and also securing your PC. It supports the Windows OS and will help you optimize PC games. It has a larger driver database and that is the reason why it can update more than 3 million drivers.

Other Interesting News and Cyber Security bits:

- Should you shift left or not?
- How to tell if there is a hidden camera in your hotel room?
- Apple touts iPhone 13's privacy features, but doesn't address spyware worries



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