On April 28, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
30-Apr	151,098,552	3,178,162

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

30 April 2021

In The News This Week

Cyber-attack hackers threaten to share US police informant data

Washington DC's Metropolitan Police Department has said its computer network has been breached in a targeted cyber-attack, US media report. A ransomware group called Babuk is reportedly threatening to release sensitive data on police informants if it is not contacted within three days. The FBI is investigating the extent of the breach, US media reported, citing the Washington DC police department. Ransomware is used to scramble computer networks and steal information. Attackers target companies or organisations and can lock their systems, then demand large sums of money in return for ending the hack. Read the story here: BBC

Nvidia Warns: Severe Security Bugs in GPU Driver, vGPU Software

The gaming- and AI-friendly graphics accelerators can open the door to a range of cyberattacks.

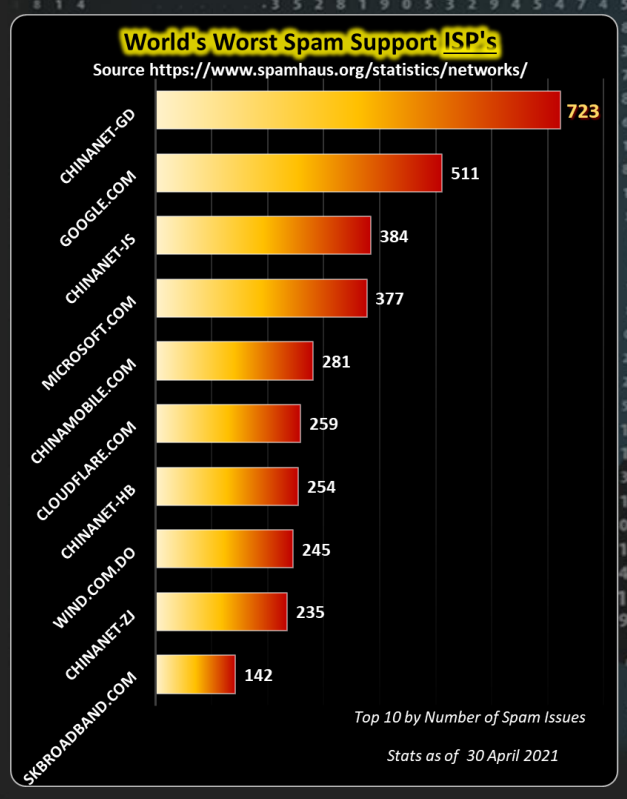
Nvidia has disclosed a group of security vulnerabilities in the Nvidia graphics processing unit (GPU) display driver, which could subject gamers and others to privilege-escalation attacks, arbitrary code execution, denial of service (DoS) and information disclosure. Meanwhile, the Nvidia virtual GPU (vGPU) software also has a group of bugs that could lead to a range of similar attacks.. Read the story by Tara Seals here: ThreatPost

Accenture acquires French cybersecurity firm Openminded

Accenture has announced its intention to acquire French cybersecurity firm Openminded. - Announced on Thursday, the services and consultancy company said the purchase will expand the Accenture security arm's presence in France and into Europe as a whole. Financial terms of the deal were not disclosed.
Founded in 2008, Openminded provides cybersecurity services including management, consultancy, and cloud & infrastructure solutions with a focus on risk analysis, remediation, and regulatory compliance. Openminded reported a €19 million turnover during the 2020 financial year. The company has roughly 105 employees and 120 clients including Sephora, Talan, and Thales. Once the deal has been finalized, Openminded's staff will join Accenture Security's existing workforce. "Joining forces with Accenture is a great opportunity for our teams and our clients," commented Hervé Rousseau, Openminded founder and CEO. "The alliance of our talent and capabilities perfectly leverages our expertise and would allow us to deliver on a global scale. Today, the fight against cyberattacks requires the implementation of the most advanced technologies, as well as the human resources to make them efficient." Read the full story here: ZDNet

Space Command to launch Joint Cyber Center

A critical part of defending SATCOM is building mesh networks to ensure system resilience in the event one part of the network is attacked. The unified combatant command overseeing the military's joint operations in space is working to stand up a Joint Cyber Center, its commander told senators Tuesday.
U.S. military branches are directing resources to the cyber center, which will look to ensure the cybersecurity of satellites and space-based communications, said Gen. James Dickinson, the Army general in charge of Space Command. Dickinson said the center will be a critical part of the command's mission and act as a central unit that can help it integrate with other cyber-focused commands, like U.S. Cyber Command.
"We are in competition each day, both in space and cyber," he told the Senate Armed Services Committee during a hearing on the fiscal 2022 defense budget request.
While the larger command is focused on space operations, it already has three general officers focused on cyberspace, Dickinson said. He repeatedly responded to questions about the security of satellite-based communications saying he has plenty of cyber capabilities to protect them but it is important to integrate operations across the military. The joint center will serve as a key part of that integration.
Read the full story here: FEDSCOOP, Military&Aerospace



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

Hacktivism

Wikipedia describes hacktivism as follows – "Activism, hacktivism, or hactivism, is the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change". Many other definitions can be found online but most of them point out that hacktivism is mostly a collaborative group effort with a clear and distinct objective and target area. As far as we know, the word "hacktivism" was first coined in 1996 by "Omega", a member of the hacker collective named Cult of the Dead Cow (cDc). A typical hacktivist campaign consists of 4 parts: (1) **Recruitment** - promoting the cause and recruiting participants for the campaign. (2) **Reconnaissance** – identifying the target and weaknesses to exploit for maximum effect. (3) **Execution** – running the carefully planned campaign. (4) **Disbandment** – disband the group and disappear until the next campaign is planned.

What is the difference between a hacker and a hacktivist?
A hacker's motive is primarily financial gain where a hacktivist's motivation is primarily social change. Now, some would say that state-sponsored attacks, like the recent SolarWinds incident, fall under the banner of hacktivism because of its political agenda. But for me, that falls under a different category of hacking that borders on cold war tactics and in the bigger scheme of things, forms only a small percentage of hack activity.

Typical techniques of the hacktivist:

- **DDoS Attacks** - Distributed denial-of-service attacks target mostly websites and online services. The aim is to overwhelm them with more traffic than the server or network can handle or what it is designed for. The goal is to render the website or service inoperable. The traffic can consist of incoming messages, requests for connections, fake packets, and so on.
- **Website Defacement** – Changing the visual appearance of a website and therefore compromise the integrity of its data. Trend Micro describes Website defacement as "similar to drawing graffiti on a wall, only it happens virtually. Websites' appearance change - pictures and/or words are scrawled across the defaced website." The aim is to make a point that promotes or drives home their cause or purpose of the protest or viewpoint.
- **Doxxing** – "Doxing or doxxing is the act of publicly revealing previously private personal information about an individual or organization" (Wikipedia). This is done via social media, blogs, or other internet-enabled avenues.

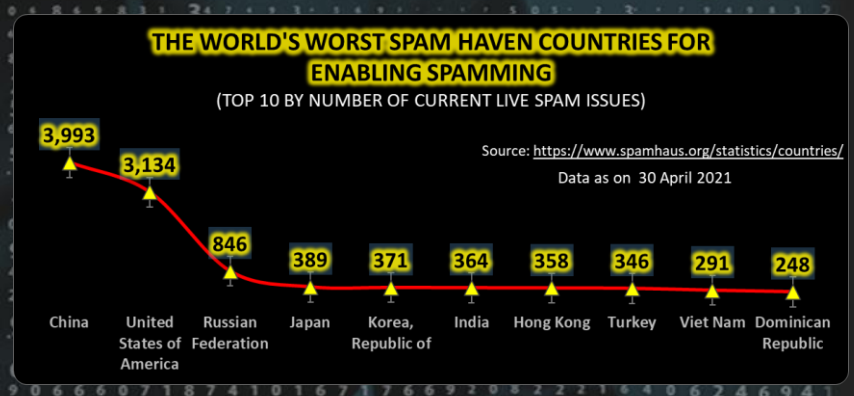
Most notable hacktivism incidents

- **1989 – Worms Against Nuclear Killers** - Computers at NASA and the U.S. Energy Department were penetrated by an anti-nuclear "WANK" worm, which altered computers' log-in screens to "WORMS AGAINST NUCLEAR KILLERS … Your System Has Been Officially WANKed." The worm was the work of a group called "The Realm" who protested against the deployment of nuclear-powered rockets and nuclear power generation in general. The campaign resulted in around half a million US dollars in damages and time lost.
- **1994 - Intervasion of the UK** - A mostly British activist group known as the Zippies launched an "email bomb" and distributed denial-of-service (DDoS) attack against British government websites to protest against Prime Minister John Major's Criminal Justice and Public Order Act, which outlawed outdoor raves featuring music with "a succession of repetitive beats." The attack, known as the "Intervasion of the UK," knocks out several government websites for more than a week. It was the first known use of DDoS — which takes down a targeted website by overwhelming it with communication requests.
- **1998 – Floodnet** – At the annual Ars Electronica Festival in Linz, Austria, a group who called themselves the "Electronic Disturbance Theater" were invited to demonstrate a program called FloodNet. Billed as a "virtual sit-in," users navigated to the FloodNet website at a predetermined time, and through a simple Java tool, were directed to a targeted website that would reload constantly every few seconds. With enough people — perhaps thousands — the sit-in caused targeted websites to slow or maybe even crash, rendering them intermittently inaccessible. The group affiliated itself with Mexico's Zapatista revolutionary movement and targeted both the Mexican and US governments.
- **1999 - Battle of Seattle** – An anti-globalization movement called the "Elecrohippies" launched a DDoS attack against the World Trade Organization (WTO) during the WTO's Ministerial Conference in Seattle, Washington. This DDoS attack blocked the computer network servicing the WTO meeting by flooding it with requests. The Elecrohippies claimed success for the action, saying 450,000 people participated over 5 days, resulting in the WTO conference network being constantly slowed and sometimes brought to a complete standstill.
- **2015/2020 – Operation DeathEaters** – The hacker collective called Anonymous launched a massive social media campaign to fight child sex abuse by targeting online pedophile networks. The campaign extended later to distribute information on influential people and their alleged involvement in child trafficking. (See Video Here)
- **2020 – Black Lives Matter** - Again, The hacker collective called Anonymous launched a campaign against police brutality and consequently hacked and temporarily disabled the Minneapolis Police Department and other government websites.
- **2021 - My Little Anonymous Revival Project** – In February this year, a hacktivist collective who calls themselves JaXpArO breached far-right social media platform Gab, pulling out 70 gigabytes of data from the backend databases. The attackers obtained user profiles, private posts, and chat messages written by users that include white supremacists, supporters of the QAanon movement, neo-Nazis, and conspiracy theorists, some of whom were associated with the Capitol Hill riot on January 6. The data obtained was then "leaked " to a transparency organization called Distributed Denial of Secrets (DDoSecrets), which now makes it available to journalists and researchers upon request.

There are many more examples out there, please follow the reference links if you want to dig deeper.
References: ScienceDirect , Panda Security, Norton, Trend Micro, CSO, Foreign Policy

Other Interesting News and Cyber Security bits:

- Apple's new privacy feature will change the web. And not everyone is happy about it
- GCHQ: Dyslexic thinkers key to solving UK cyber security challenges
- University of Michigan develops computer chip with cyber security sufficient to resist hostile hackers



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