Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On March 24, the Cyber Threat Alert Level was evaluated and is remaining at Yellow (Elevated) due to the ongoing exploitation attempts observed by the MS-ISAC regarding critical vulnerabilities in versions of Microsoft Exchange servers.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
26-Mar	126,043,740	2,766,594

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

26 March 2021

In The News This Week

Swiss Cyber Security Firm Says It Accessed Servers of a SolarWinds Hacking Group

A Swiss cyber-security firm says it has accessed servers used by a hacking group tied to the SolarWinds breach, revealing details about who the attackers targeted and how they carried out their operation. The firm, PRODAFT, also said the hackers have continued with their campaign through this month. PRODAFT researchers said they were able to break into the hackers' computer infrastructure and review evidence of a massive campaign between August and March, which targeted thousands of companies and government organizations across Europe and the U.S. The aim of the hacking group, dubbed Silverfish by the researchers, was to spy on victims and steal data, according to PRODAFT's report. Read the full story by Daniele Lepido here: Insurance Journal

Taking Down Dark Web Sites May Cause Headache for Both the Bad Guys and the Good Guys - Ever since the first dark web monitoring services became available, around 2005, consumers of such services often asked – why aren't these websites being taken down? After all, the sites that comprise the dark web are platforms and tools for illegal activities. The answer, which used to satisfy most, was that these sites are intelligence sources and taking them down means that the criminals will congregate somewhere else, somewhere that may not be known to those who monitor them. These sites are intelligence sources for both law enforcement and security vendors, without them there is less intelligence to prevent fraud, recover credentials, and reveal the true identity of criminals.

Read the full article by Idan Aharoni here: SecurityWeek *(Thanks to Christo Deysel who pointed me to this story)*

New wave of 'hacktivism' adds twist to cyber-security woes

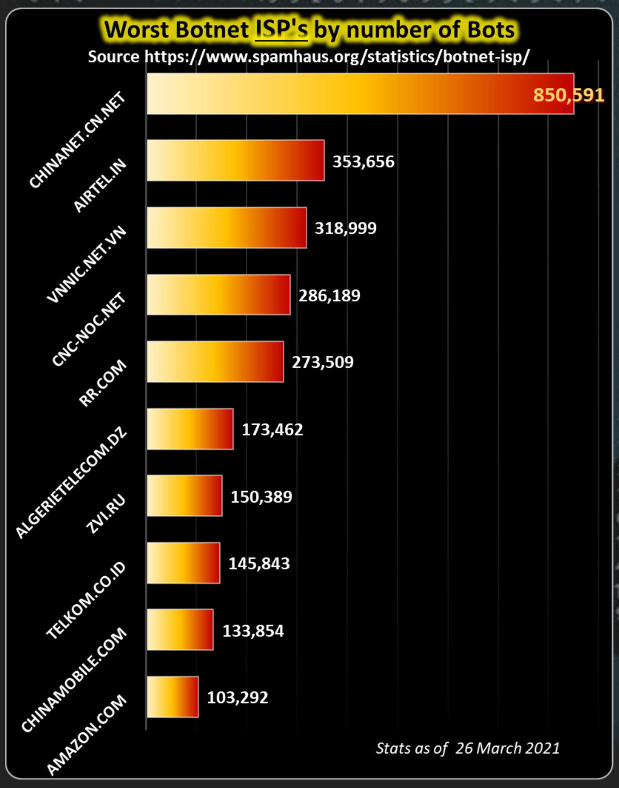
WASHINGTON (REUTERS) - At a time when US agencies and thousands of companies are fighting off major hacking campaigns originating in Russia and China, a different kind of cyber threat is re-emerging: activist hackers looking to make a political point. Three major hacks show the power of this new wave of "hacktivism" - the exposure of AI-driven video surveillance being conducted by the start-up Verkada, a collection of Jan 6 riot videos from the right-wing social network Parler, and disclosure of the Myanmar military junta's high-tech surveillance apparatus. And the US government's response shows that officials regard the return of hacktivism with alarm. An indictment last week accused 21-year-old Tillie Kottmann, a Swiss hacker who took credit for the Verkada breach, of a broad conspiracy. Read the full article here: StraitsTimes

'Black Kingdom' Ransomware Hits Unpatched Exchange Servers

Attackers gunning for an easy payday are continuing to target Microsoft Exchange servers that have not yet been updated with critical patches. On March 18, security experts began warning that a new strain of ransomware had begun targeting Exchange email servers that have not yet been updated with the patch Microsoft issued on March 2 for a ProxyLogon flaw in Exchange. The new crypto-locking malware, called Black Kingdom, has been branded "rudimentary and amateurish" by Mark Loman, director of engineering at security firm Sophos, who says it appears to have been dashed off by a "motivated script-kiddie." Black Kingdom may rank as a minor problem but security firms have warned of a surge in attack attempts - and thousands of victims - as **more than a dozen groups have already been targeting the flaws**, with some doing so as early as January - before the vulnerabilities were public knowledge. As a result, even once organizations have patched the flaws, they must still review their infrastructure for signs that they had already been compromised (see: Microsoft Exchange: Server Attack Attempts Skyrocket). Read the story by Mathew J. Schwartz here: BankInfo Security

30 million Americans affected by the Astoria Company data breach

Researchers discovered the availability in the Dark Web of 30M of records of Americans affected by the Astoria Company data breach. On January 26, 2021, threat intelligence team at Nightlion Security became aware of several new breached databases being sold on the Dark0de market by the popular hacking group Shiny Hunters. The data listed for sale included 400 million Facebook users, a database allegedly containing Instagram users, and a dump allegedly containing 300 million user database from Astoria Company. The details of the Astoria Company data sale included, said to be 40 million U.S. social security numbers. Read the story by P. Paganini here: Security Affairs


Worst Botnet ISP's by number of Bots

Source https://www.spamhaus.org/statistics/botnet-isp/

ISP	Bots
CHINANET.CN.NET	850,591
AIRTEL.IN	353,656
VNNIC.NET.VN	318,999
CNC-NOC.NET	286,189
RR.COM	273,509
ALGERIETELECOM.DZ	173,462
ZVI.RU	150,389
TELKOM.CO.ID	145,843
CHINAMOBILE.COM	133,854
AMAZON.COM	103,292

Stats as of 26 March 2021

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

Pappa, my Discord account is now going to be much more secure, because Microsoft is buying it!

Hacktivism?

In a changing world with increasing social and political tension across the globe, the Internet and more specifically, hacking, has become a tool or weapon of choice for many activist groups. We call it "hacktivism" and in the last few months, I saw a steep increase in the number of hacktivism incidents reported across the world. I, therefore, decided to explore the topic a bit more to see how deep and wide the problem is.

What is Hacktivism?

According to a definition by CheckPoint, hacktivism is "derived from combining the words 'Hack' and 'Activism'. Hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. The individual who performs an act of hacktivism is said to be a hacktivist". In the Harvard thesis of Alexandra Samuel "Hacktivism and the Future of Political Participation", she defines hacktivism, as "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development". In general, Hacktivism and Internet vandalism differs from cyberterrorism as it does not pose a direct threat to the lives and livelihoods of victims. Cyberterrorism on the other hand could lead to a physical threat to human beings.

What motivates the Hacktivist?

Hacktivists can be motivated by political views, cultural or religious beliefs, national pride, or an ideology that differs from the current norm. Hacktivist can also be rallied up when a political or social event stirs up emotions and divide a group of people into two or more strong opinion camps. Activists will often use an event like this as a springboard to influence young minds to put their skills to test. I use the term "young minds" loosely as it seems that the majority of people associated with recent events are of a younger generation. However, this does not ringfence hacktivism to young people only. I believe if we dig deeper, I can imagine that in most cases the mastermind will be of a more mature age group. This is only my opinion though as my knowledge is limited and based on surface information.

Hacktivist actions that made the news

WANK - One of the earliest Hacktivists acts is probably the 1989 "WANK" worm hack (**Worms Against Nuclear Killers)**. This was before the term "Hacktivist" was even coined though. Developed by Australian hackers under the aliases of Electron and Phoenix, the worm was sent to a computer network shared by the U.S. Department of Energy and NASA, just one day before the launch of the Galileo spacecraft. At the time, public concern over the Challenger shuttle disaster remained strong, and anti-NASA protestors argued that should the Galileo crash like the Challenger, its plutonium-based modules would cause catastrophic destruction on falling back to earth. But since then the connected digital world was thrown into a tug-of-war between hackers and cybersecurity practitioners and the fight will be going on with no end in sight.

Anonymous – An unidentified group, the hacker world called Anonymous has made the news many times since it was first observed, both for good and for bad. They're largely considered the most famous hacktivist group in the world. The group is seen by many as a Batman-like vigilante of the internet. The British newspaper The Sun even went so far as to call them "the digilantes" for their efforts to retaliate against the terrorist attacks on French satirical newspaper Charlie Hebdo.

The group, which is composed of a loosely organized international network of hacktivists, has its roots in the online image-based bulletin board 4chan, which started in 2003 and is used by people all over the world. The name "Anonymous" was inspired by the perceived anonymity under which users posted on 4chan. The group distinguishes their actions by two distinct symbols, the Guy Fawkes mask and the "man without the head" image.

The most notable actions of Anonymous include: **(1)** The Minneapolis Police Department hack after the killing of George Floyd on May 25, 2020. **(2)** Operation Tunisia where they took down Government websites and aided in the revolution in 2010 and 2011. **(3)** Security firm HBGary hacked in 2011 after the head of the company Aaron Barr, said that they have infiltrated the Anonymous group. The group released a statement to Aaron Barr saying, "You brought this upon yourself. Let us teach you a lesson you'll never forget: don't mess with Anonymous." **(4)** "Project Chanology" was a protest movement against the practices of the Church of Scientology by members of Anonymous. This was in response to the Church of Scientology's attempts to remove a highly publicized interview with Scientologist Tom Cruise from the Internet in January 2008 and said it was a form of censorship. Anonymous launched DDoS attacks and other harassing actions against the organization. – The list goes on and you can see some of them here.

"JaXpArO and My Little Anonymous Revival Project" – More recently, at the beginning of March 2021, Right-wing social media website Gab announced that they were hacked by a Hacktivist who calls himself "JaXpArO and My Little Anonymous Revival Project". His name reveals an obvious connotation to the Anonymous group. Private messages from some 15,000 Gab users were used to create a dataset of more than 40 million posts from the site, including private posts and user profiles. The hacker reportedly used a SQL injection vulnerability to siphon some 70GB of data. Activist data transparency group Distributed Denial of Secrets (DDoSecrets), plans to share the data with researchers and journalists but says it is not releasing it publicly due to privacy concerns.

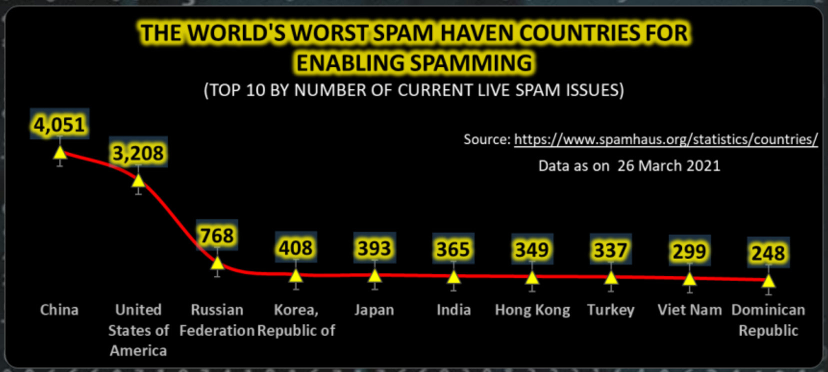
Tillie Kottmann – Kottmann, seemingly also riding on the coattails of Anonymous, is taking credit for the recent breach of a massive trove of security-camera data collected by Silicon Valley start-up Verkada. They gained access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons, and schools. Companies whose footage was exposed include carmaker Tesla, women's health clinics, psychiatric hospitals, and the offices of Verkada itself. The publication The Straits Times quoted that Kottmann said their reasons for hacking are "lots of curiosity, fighting for freedom of information and against intellectual property, a huge dose of anti-capitalism, a hint of anarchism - and it's also just too much fun not to do it". After Kottmann publicly took credit for breaching Verkada and posted alarming videos that Swiss authorities raided their home at the request of the US government.

Many more examples can be posted but that is all I have space for in this bulletin. To read more, please follow the links in the source list below.

Sources: Bustle, ScienceDirect, The Verge, BBC, Security Boulevard, News18, The Straits Times

Other Interesting News and Cyber Security bits:

- Three billion phishing emails are sent every day. But one change could make life much harder for scammers.
- The Cyber Security Breaches Survey – 2021
- Microsoft Is in Exclusive Talks to Acquire Discord


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)

Source: https://www.spamhaus.org/statistics/countries/

Data as on 26 March 2021

Country	Live spam issues
China	4,051
United States of America	3,208
Russian Federation	768
Korea, Republic of	408
Japan	393
India	365
Hong Kong	349
Turkey	337
Viet Nam	299
Dominican Republic	248

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