On March 2, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mitel and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
04 Mar 22	442,525,364	6,003,031

Deaths this week: 54,998

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
04 March 2022

In The News This Week

Anonymous sends blunt message to Vladimir Putin over invasion of Ukraine

The hacker group Anonymous has issued a message to the Russian president (Credits: Twitter, See Video here) Anonymous has sent a stark message to Vladimir Putin as the invasion in Ukraine intensifies. In recent days the hacker collective has declared all out cyberwar against Russia and already claimed to have leaked a Russian MoD database. Now the group has posted a video to Twitter addressing the Russian president directly. A person clad in the usual Guy Fawkes mask, speaking in a voice disguised by computer manipulation, addresses the camera directly, telling Putin: 'Your regime has no respect for human rights or the self determination of your neighbors.' The figure goes on to detail the horrific damage and displacement the invasion has created and the resulting refugee crisis for the people of Ukraine. 'You are the instigator,' the figure says, as footage of the invasion is played. 'You have criticized the US military and NATO for their occupation and bombardment of the middle east, which is certainly a fair criticism. 'But you have shown that you are no better than the imperialist governments that you criticize, and the whole world can see through your propaganda.' …
Read the rest of the story by Jeff Parsons here: Metro

Russian Media Sites Hacked; Anonymous Claims Responsibility

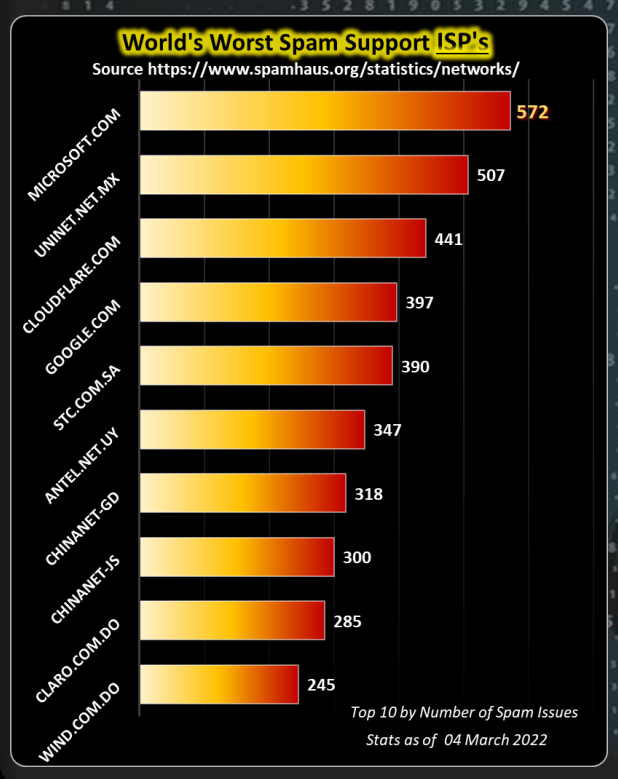
Many Russian media outlets have been hacked, with anti-war messages being placed on their websites, as Russia continues its massive, unprovoked attack on Ukraine. Twitter accounts historically associated with Anonymous, the amorphous online activist community that first grabbed global attention about a decade ago, claimed it was behind the hacker attack. Among the media outlets impacted were websites of such news agencies and newspapers as TASS, Kommersant, Izvestia, Fontanka, Forbes, and RBK. "[Russian President Vladimir] Putin forces you to lie and puts you in danger. Why do we need it? So that Putin was added to textbooks? This is not our war, let's stop him!" one of the messages read. "This statement will be removed, and some of us will be fired or even jailed. But we cannot stand it anymore," the statement signed by "Not indifferent journalists" said...
Read more here: Voanews

Anonymous hackers troll Putin by renaming his ₹729 crore yacht, sending it to hell

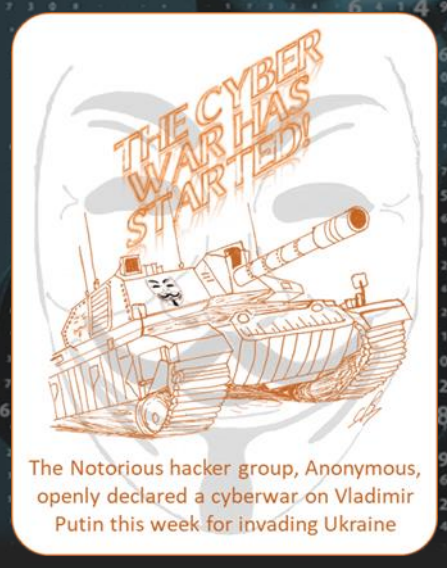
The world's largest hacker and activist collective 'Anonymous' has renamed Russian President Vladimir Putin's yacht, breaking into maritime tracking data. The vigilante group had recently announced that it is "officially in cyber war" against the Russian government. In their latest move targeting Russia, they gained access to the Automatic Identification System used to identify, locate and monitor vessels, and changed the name of Putin's $97 million (₹729 crore) yacht from 'Graceful' to 'FCKPTN'. Anonymous topped it off by renaming its destination to 'anonymous', then 'annoleaks' and eventually set it to 'hell'... Read the rest of the article here: TimesNowNews

Ukraine is building an 'IT army' of volunteers, something that's never been tried before

Ukraine has created what is describes as an "IT army" to defend against Russian hackers and to launch counter operations against cyber threats. Russia's invasion of Ukraine has been accompanied by cyberattacks targeting the country's services and infrastructure, including DDoS attacks and destructive wiper malware campaigns – leading to the Ukrainian government calling for volunteers to aid with cybersecurity. But it has also asked for support in conducting offensive cyber operations back at Russia. "We are creating an IT army," Mykhailo Fedorov, vice prime minister of Ukraine said in a tweet at the weekend. "There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists," he added, alongside a Telegram link to join the 'IT Army of Ukraine', which now has tens of thousands of subscribers.
In addition to helping to protect Ukrainian critical infrastructure and services from attacks, supporters were provided with a list of websites of 31 Russian targets. They include organisations in both the state-backed and private sectors, including government agencies, banks, critical infrastructure and energy providers, including Gazprom and Lukoil, as well Russian email provider and search engine, Yandex. The list of targets is also being circulated in some underground forums. Read more here: ZDNet



For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



The Notorious hacker group, Anonymous, openly declared a cyberwar on Vladimir Putin this week for invading Ukraine

Additional News & Articles

With the Russian invasion of Ukraine and the overwhelming response of the Cyber world, there is so much happening that I decided to dedicate the article section of this week's post to highlight more news and articles in the cyber security space.

How security vendors are aiding Ukraine

Since Russia launched a full-scale military invasion into Ukraine on February 23, a series of cyberattacks have been detected targeting Ukrainian businesses, websites and government agencies amid the ongoing conflict. Meanwhile, organizations in the cybersecurity sector have begun taking action to provide help and support to those directly and subsequently impacted by cyber incidents relating to the Ukraine-Russia crisis. Here is a list of the cybersecurity vendors currently known to be offering aid: Vectra AI, SentinelOne, Bitdefender, CrowdStrike, Microsoft, Cloudflare, Lookout & SafeBreach.
Read the rest of the article by Michael Hill here: CSO

Tech companies turn the screws on Russia

Business software giant Oracle has suspended all operations in Russia, while rival SAP has announced it will pause all sales in the country following Moscow's invasion of Ukraine. Oracle's announcement on Twitter on Wednesday came about three hours after Ukraine's minister of digital transformation tweeted at the two companies asking for support. Oracle did not respond to requests for comment to elaborate on its tweet, which said the company "has already suspended all operations in the Russian Federation". SAP in a blog post on Tuesday called economic sanctions against Russia "an important mechanism in the efforts to restore peace". "We are stopping business in Russia aligned with sanctions and, in addition, pausing all sales of SAP services and products in Russia," CEO Christian Klein wrote. He said that in addition to an initial €1-million in humanitarian support toward Ukraine, SAP had "also offered to convert our office space at locations across Europe into warehousing and accommodation for refugees".
Meanwhile, Spotify said on Wednesday it has closed its office in Russia indefinitely in response to what the audio streaming platform described as Moscow's "unprovoked attack on Ukraine". Read the rest of the article by Michael Hill here: TechCentral

Russia Releases List of IPs, Domains Attacking Its Infrastructure with DDoS Attacks

As the ongoing Russia-Ukraine conflict continues to escalate, the Russian government on Thursday released a massive list containing 17,576 IP addresses and 166 domains that it said are behind a series of distributed denial-of-service (DDoS) attacks aimed at its domestic infrastructure. Some of the noticeable domains in the listing released by Russia's National Coordination Center for Computer Incidents (NCCCI) included the U.S. Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and websites of several media publications such as the USA Today, 24News.ge, megatv.ge, and Ukraine's Korrespondent magazine. As part of its recommendations to counter the DDoS attacks, the agency is urging organizations to ringfence network devices, enable logging, change passwords associated with key infrastructure elements, turn off automatic software updates, disable third-party plugins on websites, enforce data backups, and watch out for phishing attacks. … The development comes as the ground war has been complemented by a barrage of cyber attacks in the digital domain, with **hacktivist** groups and other vigilante actors backing the two countries to strike websites of government and commercial entities and leak troves of personal data.
According to global internet access watchdog NetBlocks, Russia is said to have placed extensive restrictions on Facebook access within the country, even as widespread internet outages have been reported in different parts of Ukraine such as Mariupol and Sumy. That's not all. Ukraine, which managed to amass a volunteer "IT Army" of civilian hackers from around the world, put out a new set of targets that includes the Belarusian railway network, Russia's homegrown satellite-based global navigation system GLONASS, and telecom operators like MTS and Beeline… Read the story by Ravie Lakshmanan here: The Hacker News

Conti Ransomware Gang's Internal Chats Leaked Online After Siding With Russia

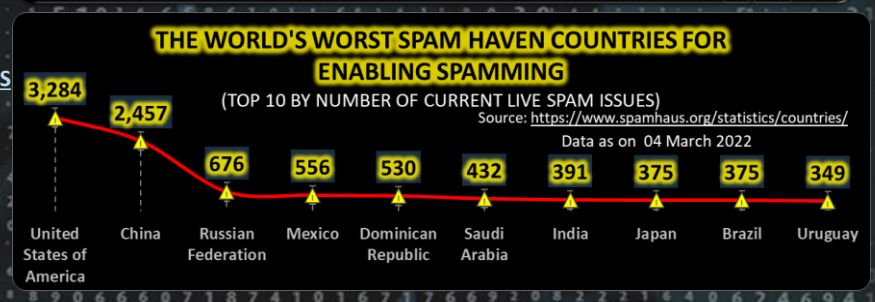
Days after the Conti ransomware group broadcasted a pro-Russian message pledging its allegiance to Vladimir Putin's ongoing invasion of Ukraine, an anonymous security researcher using the Twitter handle @ContiLeaks has leaked the syndicate's internal chats. The file dump, published by malware research group VX-Underground, is said to contain 13 months of chat logs between affiliates and administrators of the Russia-affiliated ransomware group from June 2020 to February 2022, in a move that's expected to offer unprecedented insight into the criminal enterprise's inner workings. "Glory to Ukraine," the leaker said in their message. The shared conversations show that Conti used fake front companies to attempt to schedule product demos with security firms like CarbonBlack and Sophos to obtain code signing certificates, with the operators working in scrum sprints to complete the software development tasks. Read the story by Ravie Lakshmanan here: The Hacker News

Toyota forced to stop vehicle production in Japan due to Cyberattack

Toyota's production facilities in Japan have been brought to a halt o Wednesday. According to Nikkei, one of Toyota's most key suppliers has been hacked in some way, though Toyota has been tight-lipped about the details. "Due to a system failure at a domestic supplier (Kojima Industries Corporation), we have decided to suspend the operation of 28 lines at 14 plants in Japan on Tuesday, March 1st (both 1st and 2nd shifts), according to on its website. The "system failure," according to a Kojima Industries official, was actually a hack against Nikkei. "We have been struck by some form of cyberattack," a source close to Kojima confirmed. They are confirming and verifying the damage and are moving quickly to respond, with the top priority being to get Toyota's production system back up and running as soon as possible." The cyberattack's details are still hazy at best — and not because either firm is trying to hide them. Kojima said yesterday that it was still trying to figure out what kind of malware was used in the attack, as well as establishing out who the attacker was and how much damage had been done to its networks.
Read the rest of the article by Srestha Roy here: TechStory

Other Interesting News and Cyber Security bits:

- Fightback against Putin's propaganda machine
- Hackers Who Broke Into NVIDIA's Network Leak DLSS Source Code Online
- SANS Daily Network Security Podcast (Stormcast)



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