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

On February 23, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
25 Feb 22	432,004,236	5,948,033

Deaths this week: 64,267

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

25 February 2022

In The News This Week

Flight tracker Flightradar24 crash caused by 'international interest' in Ukraine, Russia conflict - At the time of writing, the Flightradar24 website displays a 'cancelled' message and it is not possible to access the service. Flightradar24 is a popular tracker to monitor flights in real-time, including commercial trips, freight, repatriation flights, and now, potentially military aircraft. On Thursday, as Russian forces invaded Ukraine, Flightradar24 has experienced traffic rates 10 - 20 times higher than normal. "Due to extremely heavy load, some users may experience slowness or temporary connection issues accessing Flightradar24," the organization says. "We're working on increasing available performance now." "We are still working hard on increasing the capacity, but the very big international interest generate[s] 10-20 times higher traffic than normal, which is hard to handle. Read the rest of the story by Charlie Osborne here: ZDNet

Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities

As Ukrainian cities come under air attack from Russian forces, the country has also suffered the latest blows in an ongoing campaign of cyber attacks. Several of Ukraine's bank and government department websites crashed on Wednesday, the BBC reports. The incident follows a similar attack just over a week ago, in which some 70 Ukrainian government websites crashed. Ukraine and the United States squarely blamed Russia. With a full-scale invasion now evident, Ukraine can expect to contend soon with more cyber attacks. These have the potential to cripple infrastructure, affecting water, electricity and telecommunication services – further debilitating Ukraine as it attempts to contend with Russian military aggression. Cyber attacks fall under the traditional attack categories of sabotage, espionage and subversion. They can be carried out more rapidly than standard weapon attacks, and largely remove barriers of time and distance. Launching them is relatively cheap and simple, but defending against them is increasingly costly and difficult.. Read more here: The Conversation

New Wiper Malware Targeting Ukraine Amid Russia's Military Operation

Cybersecurity firms ESET and Broadcom's Symantec said they discovered a new data wiper malware used in fresh attacks against hundreds of machines in Ukraine, as Russian forces formally launched a full-scale military operation against the country. The Slovak company dubbed the wiper "HermeticWiper" (aka KillDisk.NCV), with one of the malware samples compiled on December 28, 2021, implying that preparations for the attacks may have been underway for nearly two months. "The wiper binary is signed using a code signing certificate issued to Hermetica Digital Ltd," ESET said in a series of tweets. "The wiper abuses legitimate drivers from the EaseUS Partition Master software in order to corrupt data. As a final step the wiper reboots [the] computer..

Read the rest of the article by Ravie Lakshmanan here: The Hacker News

Police arrest underage boys for data breach at school community

The Netherlands - Agents arrested two underage boys last week on suspicion of involvement in a data breach at a school community in Drachten, Friesland. The personal details of more than a thousand students were made public, the police reported Monday. The school community reported the data breach on January 20. The two suspects are students from the school community. The duo are suspected of computer breaches, data theft and data distribution. They have since been released, but remain a suspect in the case, according to police. nu.nl

Xenomorph Malware Burrows into Google Play Users, No Facehugger Required

New banking trojan with ties to Cerberus and Alien discovered. An Android trojan dubbed Xenomorph has nested in Google Play, already racking up more than 50,000 downloads from the official app store. For anyone who downloaded the "Fast Cleaner" app, it's time to nuke it from orbit. According to a ThreatFabric analysis, Xenomorph has a target list of 56 different European banks, for which it provides convincing facsimiles of log-in pages whenever a victim attempts to log into a mobile banking app. The goal of course is to steal any credentials that victims enter into the faux log-in overlay. However, the malware is also a flexible, modular banking trojan, which has code overlaps and other ties to the Alien malware – hence the name.

Read the rest of the article by Tara Seals here: ThreatPost

Ukraine invasion: How a digital cold war with Russia threatens the IT industry?

The Russian invasion of Ukraine is front and center on every news channel this week, and predictions of an imminent war with NATO Allies paint a bleak picture. But, what does that mean for us in the Cyberworld? ZDNet posted an article this week, written by Jason Perlow, that looks into the possible impact the conflict can have on the cyber world. Below is a condensed version of Jason's article.

Jason Perlow wrote – "In the five years since I first explored the potential impact of a Digital Cold War on the IT industry, tensions with Russia have gotten worse, especially following a series of cyberattacks on systems in the United States. These include Russia's involvement in the SolarWinds breach, as well as its interference with the 2016 US presidential elections via attacks on the Democratic National Committee infrastructure and the purchasing of tens of millions of ads on Facebook in an attempt to sow discontent among US voters. Under Vladimir Putin's leadership, the nation has focused on international cybersecurity concerns for many years.

UKRAINE INVASION - Under the pretext of "Peacekeeping operations," Russia has now initiated a full-scale invasion of Ukraine. Presumably, Russia also has been responsible for recent cyberattacks on Ukrainian banks. In response, the United States, NATO nations, and allied countries have imposed numerous economic sanctions on Russia, including blocking its two state-owned banks from debt trading on US and European markets and freezing their assets under US jurisdictions, as well as freezing the assets of the country's wealthiest citizens. Germany has halted its plans on Russia's Nord Stream 2 Gas Pipeline. Further wide-ranging sanctions are expected as Russia continues its assault on Ukraine. An extended conflict with Russia -- coupled with the imposition of wide-ranging sanctions -- will have a tangible impact on the global technology industry.

RUSSIAN TECH FIRMS ARE NOW 'TECHNOLOGIA NON GRATA' WITHIN ENTERPRISES IN WESTERN NATIONS - Let's start with Russian software companies themselves. Many of these have significant market share and widespread use within US corporations. Some of these were founded in Russia, while others are headquartered elsewhere but maintain a significant amount of their development presence within Russia and other parts of Eastern Europe. UK-incorporated Kaspersky Lab, for example, is a major and well-established player in the antivirus/antimalware space. It maintains its international headquarters, and has substantial research and development capabilities in Russia, even though its primary R&D center was moved to Israel in 2017. It's also thought that Eugene Kaspersky, the company's founder, has strong personal ties to the Putin-controlled government. Kaspersky has repeatedly denied these allegations, but questions about the man and his company remain and will be further scrutinized, particularly as the conflict develops. In the past, evidence emerged that Kaspersky's software was involved in compromising the security of a contract employee of the United States National Security Agency in 2015.

NGINX Inc is the support and consulting arm of an open source reverse proxy web server project that is very popular with some of the most high-volume internet services on the planet. The company is of Russian origin but was sold to F5 Networks in 2019. The founder of the company, Igor Sysoev, announced his departure in January of this year.

Parallels, Inc., which Corel acquired in 2018, focuses extensively on virtualization technology. Their Parallels Desktop is one of the most popular solutions for Windows virtualization on the Mac. Historically, their primary development labs were in Moscow and Novosibirsk, Russia. The company was founded by a Russian, Serguei Beloussov (who became a Singaporean citizen in 2001), and has many persons of Russian origin as key developers and executives.

Acronis, like Parallels, is another company founded by Serguei Beloussov. After founding Parallels in 1999, and being involved with both companies for some time, he became CEO of Acronis in May of 2013. The company specializes in cybersecurity products for end-to-end device protection, and in the past, has had bare-metal systems imaging, systems deployment, and storage management products for Microsoft Windows and Linux.

Veeam Software founded by Russian-born Ratmir Timashev concentrates on enterprise backup solutions for VMware and Microsoft public and private cloud stacks. Like Parallels and Acronis, it is also multinational. For many years, it had much of its R&D based out of St. Petersburg, Russia. It was purchased by Insight Partners in 2020 and installed a new management team. However, it has yet to be determined how much Russian legacy code is in its products or continues to be contributed to them.

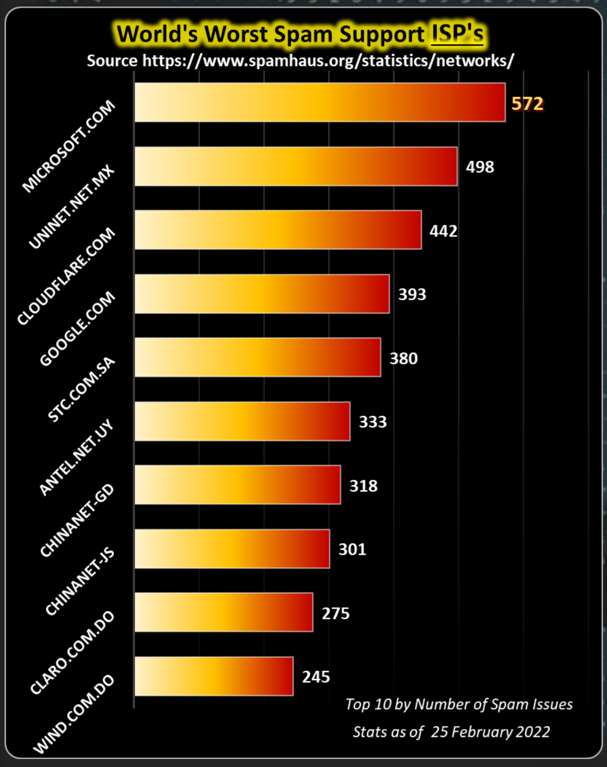
These are only just a few examples. Numerous Russian software firms generate billions of dollars of revenue that have products and services that have significant enterprise penetration in the United States, EMEA, and Asia. There are also many smaller ones that perform niche or specialized services. It should also be noted that many mobile apps -- including entertainment software for iOS, Android, Windows -- also originate in Russia.

RUSSIAN SERVICES FIRMS WILL ALSO BE IMPACTED - Many global technology giants in the software and services industries have used Russian and Eastern European developers in the past because of their high-quality and value-priced work compared to their US and Western Europe-based counterparts. And many have invested hundreds of millions of dollars in having a developer as well as reseller channel presence in Russia. The escalation into full-blown conflict in Ukraine will make C-seats within global enterprises extremely concerned about using software that originates from Russia or has been produced by Russian nationals. The most conservative companies will probably "rip and replace" most off-the-shelf stuff and go with other solutions, preferably American ones. The Russian mobile apps? BYOD mobile device management (MDM) policies will wall them off from being installed on any device that can access a corporate network. And if sanctions are put in place by world governments, we can expect them to disappear entirely from the mobile device stores. Countless games and apps originating from Russia could be no more when actual sanctions on that industry are implemented.

Please find the full article here: ZDNet

World's Worst Spam Support ISP's

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



Top 10 by Number of Spam Issues

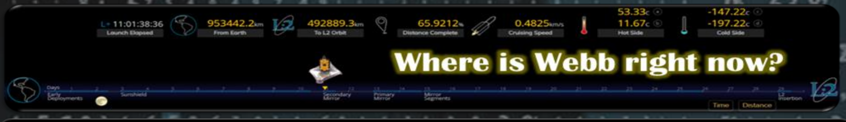
Stats as of 25 February 2022

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

Experts predict that the Ukraine crisis could spill over into a full-on cyber war that will hurt the rest of the world.

Other Interesting News and Cyber Security bits:

- Ukraine conflict ignites fears over cyberwarfare
- 'This is rocket science': micrometeorite collision blamed for NBN satellite internet outage
- SANS Daily Network Security Podcast (Stormcast)

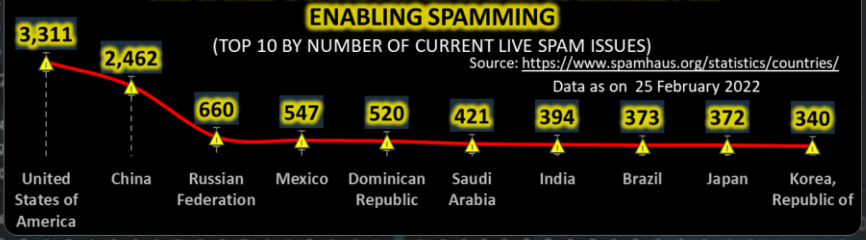


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)

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

Data as on 25 February 2022



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