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

On March 28, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, and WordPress products. This level still remains. On April 2, 2019 an advisory were released for Multiple Vulnerabilities in Google Android OS that Could Allow for Remote Code Execution

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

12 April 2019

In The News This Week

Famous hacker, Julian Assange evicted from Ecuadorian embassy and arrested.

Julian Assange was evicted from Ecuadorian embassy on Thursday 11 April 2019 for 'spoiled brat' behaviour, President Lenin Moreno says. The dramatic end to Assange's asylum has sparked curiosity about his seven-year stay inside Ecuador's embassy in London that was marked by his late-night skateboarding, the physical harassment of his caretakers and even the smearing of his own faecal matter on the walls of the diplomatic mission. It would have tested the patience of any host. But for tiny Ecuador, which prides itself on its hospitality and spent almost $US1 million ($1.4 million) a year protecting Assange, it was also seen as a national insult. "We've ended the asylum of this spoiled brat," a visibly flustered President Lenin Moreno said on Thursday in a fiery speech explaining his decision to withdraw protection of Assange and hand him over to British police. "From now on we'll be more careful in giving asylum to people who are really worth it, and not miserable hackers whose only goal is to destabilise governments."

He now faces US federal conspiracy charges related to one of the largest ever leaks of government secrets. The UK will decide whether to extradite Assange, in response to allegations by the Department for Justice that he conspired with former US intelligence analyst Chelsea Manning to download classified databases. He faces up to five years in US prison if convicted on the charges of conspiracy to commit computer intrusion.

Ecuador emerged as a safe haven for the WikiLeaks founder in 2012 as his legal options to evade extradition to Sweden over sex crime accusations, which has since been dropped. On a June day, he moved into the country's embassy near the upscale Harrods department store for what most thought would be a short stay. Instead, the cramped quarters, where a small office was converted into a bedroom, became a permanent address that some likened to a de facto jail. As the asylum dragged on, his relations with his hosts soured and his behaviour became more erratic.

Julian Assange came to international attention as the founder of the whistle-blowing website WikiLeaks. Born on July 3, 1971, in Townsville, Australia, Julian Assange used his genius IQ to hack into the databases of many high-profile organizations. In 2006, Assange began work on WikiLeaks, a website intended to collect and share confidential information on an international scale. For his efforts, the internet activist earned the Time magazine "Person of the Year" title in 2010. In 2016, his work again drew international attention when WikiLeaks published thousands of emails from U.S. presidential candidate Hillary Clinton and the Democratic National Committee, an effort believed to have impacted that year's presidential election.

Story compiled from several news reports and web resources

Cyber espionage attack group adds mobile malware to its toolset.

Reports from KASPERSKY SECURITY ANALYST SUMMIT - Singapore - A cyber espionage group believed to be out of Iran and known for targeting telecommunications providers and government bodies in the Middle East has added to its arsenal malware for targeting Android devices.

The so-called MuddyWater hacking group, which has been in action since at least 2017, also has created new backdoor malware for spying on its targets and has been spotted employing false flag tactics to throw off researchers and investigators, according to security researchers at Trend Micro, who here today shared the details of the Iranian hacking team's latest activities. MuddyWater's attack campaigns to date have been focused on gaining access to telecom providers and government entities, initially via spear phishing emails. But despite all of the intel gathered on the gang's tactics, tools, payloads, and indicators of compromise, Trend Micro researchers Jaromir Horejsi and Daniel Lunghi said MuddyWater's actual endgame remains a mystery to them. Read the full story at https://www.darkreading.com/

EMP and Geostorms, its effects on our electronic world

EMP attacks or natural EMP phenomena and its consequent disruptive effects on electronic and computing systems has been the topic of many social media discussions and news reports recently. It even made it into the gaming world, as it is included as a major weapon in a popular computer game, and also the movies.

What Is EMP?

EMP stands for electromagnetic pulse, which is considered a short burst of electromagnetic radiation. This kind of burst can come from a variety of sources, including our own sun, lightning strikes, etc. but in the case of a man-made attack, we're talking about a pulse from a nuclear detonation that occurs at an extremely high altitude. When a nuclear explosion occurs in space above a target, three types of electromagnetic pulses follow: E1, E2, and E3. An E1 pulse involves high-energy gamma rays colliding with air molecules nearly 20 miles above, then raining down electrons that get pulled in by Earth's natural magnetic field. An E2 pulse comes from high-energy neutrons that get fired in every direction, and an E3 pulse occurs due to the size of the nuclear fireball itself affecting the Earth's magnetic field. As nuclear physicist Dr. Yousaf Butt explains, these pulses affect everything in line of sight of the nuclear blast. For example, a blast at 60 miles up can affect a 700-mile radius on Earth. However, there is a "safe space" that is unaffected by all three pulses almost directly below the blast thanks to the Earth's magnetic field.

What does that mean to us?

EMP bombs do not cause casualties directly. The blast happens much too far away from people. Their power comes from interfering, disrupting, or damaging electronic equipment. That could mean power grids going down, cars and planes losing power, computer systems going berserk, and possibly even losing emergency backup power at facilities like hospitals. It sounds pretty scary, and EMP blasts are a significant threat, but the effects are largely untested and exaggerated through pop culture and inflammatory claims by politicians.

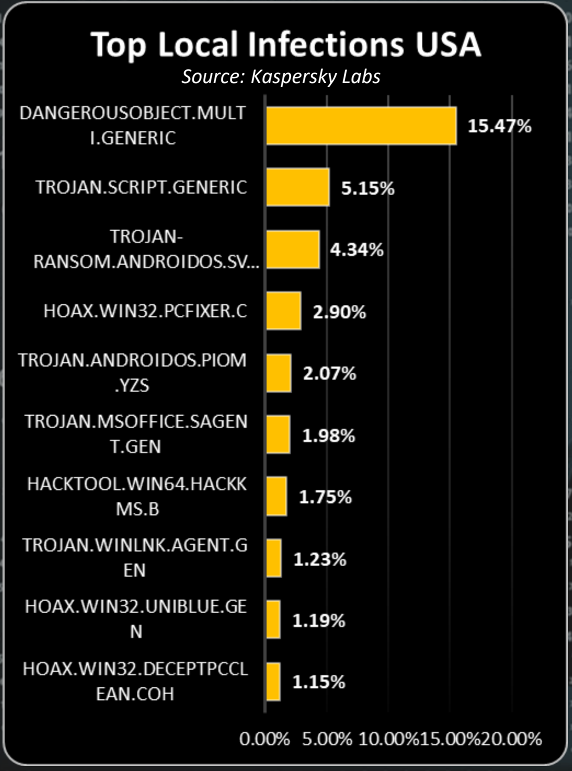
Still, we are certain about some aspects of nuclear-based EMP detonations. According to Dr. Butt, each of the three different types of pulse—E1, E2, and E3—affect various types of electrical systems in different ways. E1 affects local antennas, short cable runs, equipment inside buildings, integrated circuits, sensors, communication systems, protective systems, and computers; E2 is similar to a lightning strike (so not as damaging since we know how to deal with it), and affects longer conductive lines, vertical antenna towers, and aircraft with trailing wire antennas; and E3 affects power lines and long communications lines like undersea and underground cables, which could wreak havoc on commercial power and landlines. Overall, most of the damage would come from E1 and E3 pulses disrupting the technology we've come to rely on. Post-blast, generators may be able to still provide power, but for the most part, people would not have access to electricity. This could be devastating, or it could be extremely inconvenient until it's fixed—it's all speculation.

EMP in History

The first recorded damage from an electromagnetic pulse came with the solar storm of August 1859, or the Carrington Event. It was the largest solar storm in recorded history. Sunspots and flares could be seen on the sun and was followed by a huge geomagnetic storm. A similar, but milder, storm occurred in March 1989. It knocked out power supplies in Quebec, jammed radio signals and weather satellites and caused aurora as far south as Texas. In July 2012, Nasa reported an extreme solar storm that barely missed the earth and could have had devastating effects. Also, in August 2013, the Washington Post reported a "near miss" as massive sun flares were observed that could have knocked us out.

The phenomenon of electromagnetic interference was noticed during the early nuclear tests in the Cold War. British scientists attributed instrumentation failures to what they dubbed 'radioflash'. Its potential as a weapon was first realised by the US military. In the Starfish Prime test in 1962 a 1.44 megaton warhead was donated 250 miles into space. The pulse knocked out street lights and damaged telephones on Hawaii.

Compiled from several online resources including:
https://lifehacker.com/
https://www.washingtonpost.com
https://www.nasa.gov/

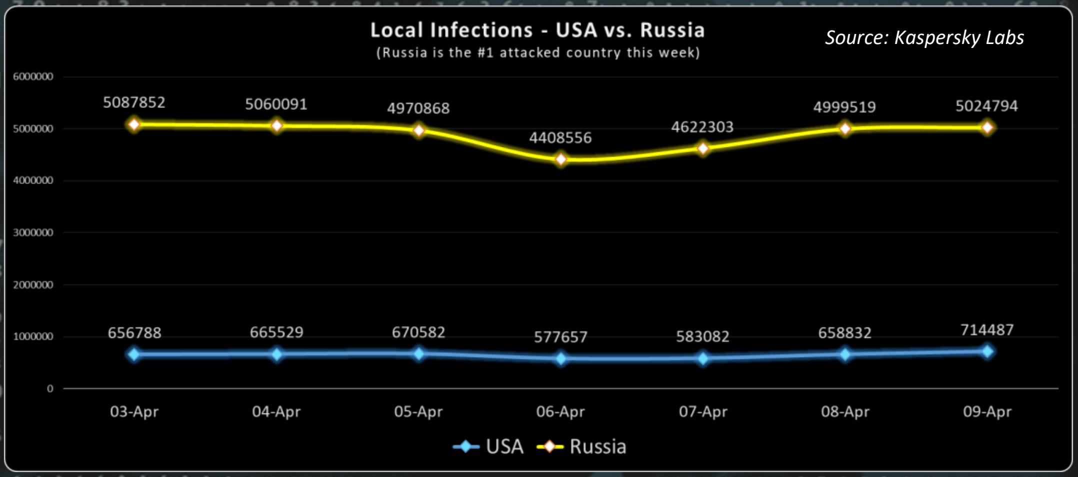


Top Local Infections USA

Source: Kaspersky Labs

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

Cybersecurity Ventures Reports:
Nearly
60 million
Americans were affected by
identity theft in 2018 as per an online survey by The Harris Poll



Local Infections - USA vs. Russia

(Russia is the #1 attacked country this week)

Source: Kaspersky Labs

Author: Chris Bester