On April 13, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in VMware, FortiWAN, Google, Microsoft, Adobe, and Citrix products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
14 Apr 22	502,183,962	6,214,494

Deaths this week: 18,348

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 – EASTER EDITION

15 April 2022

In The News This Week

US federal alert warns of the discovery of malicious cyber tools

Multiple US government agencies issued a joint alert Wednesday warning of the discovery of malicious cyber tools created by unnamed advanced threat actors that they said were capable of gaining "full system access" to multiple industrial control systems. The public alert from the Energy and Homeland Security departments, the FBI and National Security Agency did not name the actors or offer details on the find. But their private sector cybersecurity partners said the evidence suggests Russia is behind the tools – and that they were configured to initially target North American energy concerns. Read the full story here: The Guardian

Western Hackers Used Russia's Own Ransomware Against It In Cyberattack on Russia's Space Agency Roscosmos: Report

Nearly a month after a cyberattack on Russia's space agency Roscosmos, it has been revealed that the hackers used Kremlin's own medicine against them.
According to The Telegraph, hackers linked to Anonymous - Network Battalion 65 or NB65 - had revealed last month that they had stolen a bunch of files from the Roscosmos. They had stated that Russian President Vladimir Putin "no longer has control over spy satellites". To prove that they had the files, the group even shared a tweet that claimed to be Russian space agency's server information. Read the story here: NDTV

Ukrainian power grid 'lucky' to withstand Russian cyber-attack

he Ukrainian government has revealed it narrowly averted a serious cyber-attack on the country's power grid. Hackers targeted one of its largest energy companies, trying to shut down substations, which would have caused blackouts for two million people. The malicious software used in the attack is similar to that used by Russian hackers who previous caused power cuts in Kyiv. Researchers believe Russian military group Sandworm is responsible. It is the most serious cyber-attack so far launched against Ukraine since the Russian invasion.
In a press conference on Tuesday, Viktor Zhora, deputy chairman of the State Service of Special Communications, said his team were alerted to a possible attack on energy grids at the beginning of the invasion of his country..
Read the rest of the story here: BBC News

Microsoft Leads Operation to Disrupt Zloader Botnet

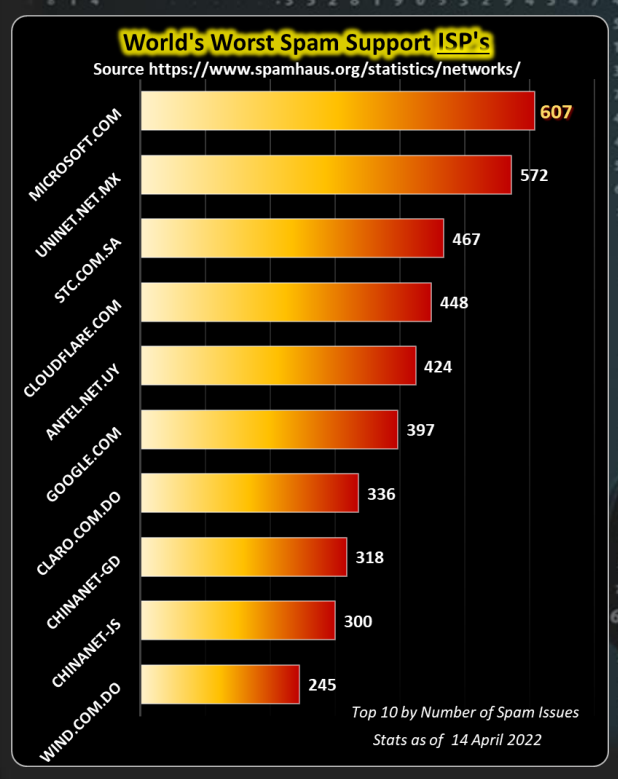
The banking Trojan-turned-ransomware-distribution tool has been a potent threat since late 2019. - Researchers from Microsoft and several security vendors have sinkholed 65 domains associated with the prolific Zloader malware distribution botnet. Another 319 backup domains that Zloader generated via an embedded domain generation algorithm (DGA) have been seized as part of the same operation, which included ESET, Palo Alto Networks, and Black Lotus Labs. The goal is to disable the infrastructure that the criminal gang behind the Zloader botnet has been using as part of its malware-distribution-as-a-service operation, says Amy Hogan-Burney, general manager of Microsoft's digital crimes unit. . Read the story here: DarkReading

Oil India suffers cyber attack, receives Rs 57 crore ransom demand

PSU major Oil India, which suffered a cyberattack disrupting its operations in Assam, has received a ransom demand of USD 75,00,000 (over Rs 57 crore) from the perpetrator, officials said on Wednesday. A case was registered under various sections of the Indian Penal Code and the Information Technology Act, 2000, after the company lodged a complaint with the police. The public sector undertaking OIL and the government exchequer have incurred a huge financial loss due to the cyberattack - ransomware, as the business through the IT system has been seriously affected, OIL Manager (Security) Sachin Kumar said in the police complaint. The cyberattack took place on April 10 at OIL's one of the workstations of the Geological and Reservoir department, but it was intimated by the IT department on Tuesday, he said. Read the story here: Business Standard

Ethereum Developer Jailed 63 Months for Helping North Korea Evade Sanctions

A U.S. court has sentenced former Ethereum developer Virgil Griffith to five years and three months in prison and pay a $100,000 fine for conspiring with North Korea to help use cryptocurrencies to circumvent sanctions imposed on the country. "There is no question North Korea poses a national security threat to our nation, and the regime has shown time and again it will stop at nothing to ignore our laws for its own benefit," U.S. Attorney Damian Williams said in a statement.... Read the story here: The Hacker News



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

Cyberbullying: What is it and how to stop it

If you have children, the topic of cyberbullying was probably discussed at some stage or came over your path and affected you directly to some degree. It is a phenomenon that grew proportionally with the digitization of our modern world. Since the Internet became available to the masses, kids and adults alike experimented with this "new" communication medium and soon discovered that they can influence or manipulate someone by the way they interact or "chat" with them. Cyberbullying comes in many forms and includes anything from harassment to physical threats. Psychologists found that teenagers are mostly affected, but the phenomenon is quite evident in younger kids too. There are many online resources available, and I'll post a few links in the "References" tab at the bottom, but I found an informative post on the UNICEF website, and I felt it worth sharing some of the questions and answers posted. So, for the parents out there, get in the know and discuss it with your kids whether you think they are bullied or not.

Cyberbullying: What is it and how can we stop it?

We brought together UNICEF specialists, international cyberbullying and child protection experts, and teamed up with Facebook, Instagram, TikTok and Twitter to answer some of the most common questions about online bullying and give advice on ways to deal with it.

What is cyberbullying?

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include: (1) spreading lies about or posting embarrassing photos or videos of someone on social media,
(2) sending hurtful, abusive or threatening messages, images or videos via messaging platforms, (3) impersonating someone and sending mean messages to others on their behalf or through fake accounts.
Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.

Am I being bullied online? How do you tell the difference between a joke and bullying?

All friends joke around with each other, but sometimes it's hard to tell if someone is just having fun or trying to hurt you, especially online. Sometimes they'll laugh it off with a "just kidding," or "don't take it so seriously."
But if you feel hurt or think others are laughing at you instead of with you, then the joke has gone too far. If it continues even after you've asked the person to stop and you are still feeling upset about it, then this could be bullying.
And when the bullying takes place online, it can result in unwanted attention from a wide range of people including strangers. Wherever it may happen, if you are not happy about it, you should not have to stand for it.
Call it what you will – if you feel bad and it doesn't stop, then it's worth getting help. Stopping cyberbullying is not just about calling out bullies, it's also about recognizing that everyone deserves respect – online and in real life.

What are the effects of cyberbullying?

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways: (1) Mentally – feeling upset, embarrassed, stupid, even afraid or angry, (2) Emotionally – feeling ashamed or losing interest in the things you love, (3) Physically – tired (loss of sleep), or experiencing symptoms like stomach aches and headaches
The feeling of being laughed at or harassed by others, can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives.
Cyberbullying can affect us in many ways. But these can be overcome and people can regain their confidence and health.

Who should I talk to if someone is bullying me online? Why is reporting important?

If you think you're being bullied, the first step is to seek help from someone you trust such as your parents, a close family member or another trusted adult. In your school you can reach out to a counsellor, the sports coach or your favourite teacher – either online or in person. And if you are not comfortable talking to someone you know, search for a helpline in your country to talk to a professional counsellor. If the bullying is happening on a social platform, consider blocking the bully and formally reporting their behaviour on the platform itself. Social media companies are obligated to keep their users safe.
It can be helpful to collect evidence – text messages and screen shots of social media posts – to show what's been going on. For bullying to stop, it needs to be identified and reporting it is key. It can also help to show the bully that their behaviour is unacceptable. If you are in immediate danger, then you should contact the police or emergency services in your country.

I'm experiencing cyberbullying, but I'm afraid to talk to my parents about it. How can I approach them?

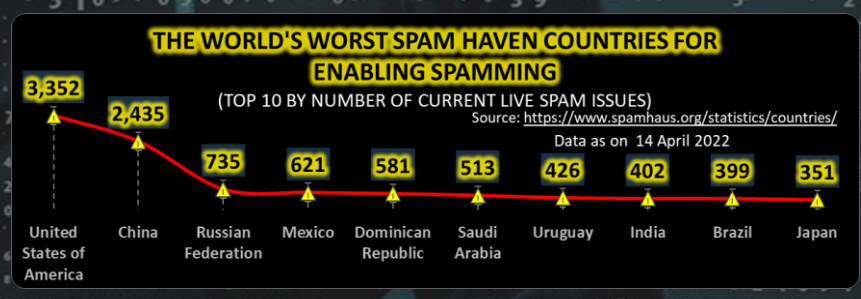
If you are experiencing cyberbullying, speaking to a trusted adult – someone you feel safe talking to – is one of the most important first steps you can take. Talking to parents isn't easy for everyone. But there are things you can do to help the conversation. Choose a time to talk when you know you have their full attention. Explain how serious the problem is for you. Remember, they might not be as familiar with technology as you are, so you might need to help them to understand what's happening.

Please visit the UNICEF site to pick up on other important questions and answers like; "How can I help my friend?" Or "Is there a punishment for Cyberbullying?" and many more.

References: ChildLine South Africa, Facebook Info, TicToc, Cyberbullying Research Center, Instagram Parents Guide, Int helpline

Other Interesting News and Cyber Security bits:

- Ukraine claims its Neptune missiles hit Russian naval flagship Moskva
- No plain sailing: modern pirates hack superyachts' cybersecurity – Dubai Boat Show
- SANS Daily Network Security Podcast (Storm cast)



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