The Cyber Threat Alert Level as evaluated by CIS remains at Blue (Guarded)

Last Advisory 28 Jul 2021

A Vulnerability in macOS Big Sur, iOS and iPadOS Could Allow for Arbitrary Code Execution

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
30 July	197,381,922	4,214,877

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

30 July 2021

In The News This Week

LockBit ransomware now encrypts Windows domains using group policies

A new version of the LockBit 2.0 ransomware has been found that automates the encryption of a Windows domain using Active Directory group policies. The LockBit ransomware operation launched in September 2019 as a ransomware-as-a-service, where threat actors are recruited to breach networks and encrypt devices. In return, the recruited affiliates earn 70-80% of a ransom payment, and the LockBit developers keep the rest. Over the years, the ransomware operation has been very active, with a representative of the gang promoting the activity and providing support on hacking forums. After ransomware topics were banned on hacking forums [1, 2], LockBit began promoting the new LockBit 2.0 ransomware-as-a-service operation on their data leak site. Included with the new version of LockBit are numerous advanced features, but 2 stands out namely: (1) Uses group policy update to encrypt network - When executed, the ransomware will create new group policies on the domain controller that are then pushed out to every device on the network. (2) LockBit 2.0 print bombs – It print bombs all networked printers with the ransom note. Read the full story by Lawrence Abrams here: Bleeping Computer

TikTok sets up cyber security hub in Dublin

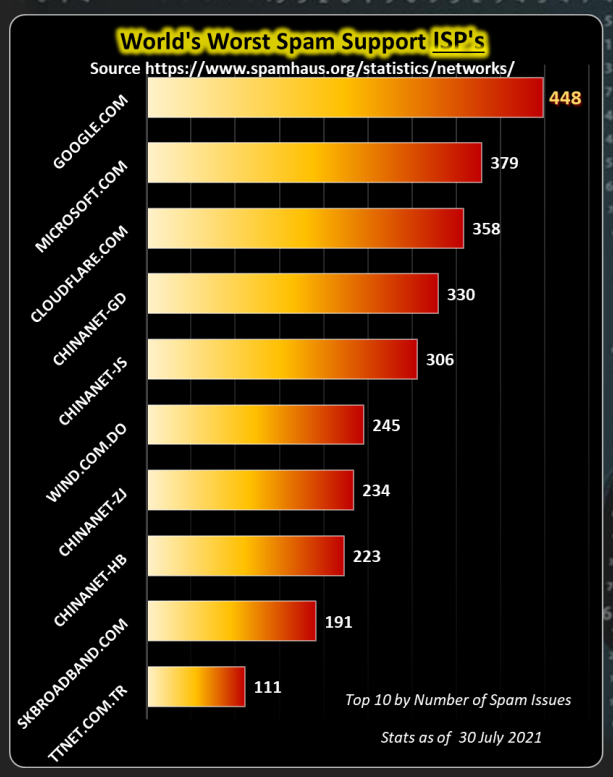
TikTok, the short-form video-sharing app that found itself the subject of global attention in 2020 when it became subject to actions against it ordered by then US president Donald Trump, is to open a new cyber security centre in Dublin. The company's new Fusion Centre builds on a November 2020 expansion in the Irish capital to oversee data protection and privacy in Europe. The centre is the second site – one already exists in Washington DC – dedicated to monitoring, response and investigative capabilities, allowing TikTok to detect and respond to critical incidents "in real time". Roland Cloutier, global chief security officer at TikTok, said: "When people use TikTok, we know they are entrusting us with their data, and we take our duty to protect that data very seriously. That's why, in developing our platform, security is built-in from the start. "Our global security organisation operates a 'follow the sun' approach so that people on teams around the world are always focused on protecting people's information – and ensuring that our next-generation entertainment platform can anticipate and stay ahead of next-generation security threats.. Read the story by Alex Scroxton here: ComputerWeekly

South Africa - Western Cape Blood Service hit by cyberattack

The Western Cape Blood Service (WCBS) was hit by a cyberattack on Thursday morning, forcing the non-profit to resort to manual, offline processing while it restores its systems from backup. WCBS spokeswoman Marike Gevers confirmed to TechCentral on Thursday that the organisation had fallen victim to a cyberattack but denied market speculation that it was a ransomware attack. "We are operating, and putting measures in place," Gevers said. "We are still restoring all our data, and the incident is being investigated by contracted experts."
She denied that the attackers were trying to extort a ransom but said information security contractors have been brought in to probe the incident and to determine what happened. "We have had to revert to a manual system and put other contingency measures in place for the donation, processing and testing of blood," she added. The blood service's systems are routinely backed up. Blood donations are continuing as normal despite the cyberattack.. Read the full story by Duncan McLeod here: TechCentral

Estonia 's police arrested a man suspected of stealing 286K ID scans from Gov. systems

Estonian police arrested a man from Tallinn that is suspected to have stolen 286,438 belonging to Estonians citizens from the government systems. The hacker exploited a vulnerability in a photo transfer service vulnerability to download ID scans from the Identity Documents Database (KMAIS). The hacker did not breach e-state services. At the time of this writing that is no evidence that the same vulnerability was exploited in the past by other threat actors. "This data was not, however, enough for the hacker to access e-state services, meaning the normal means of authentication (ID card, mobile ID and SMART ID) have not been compromised." A joint operation conducted by the cybercrime Bureau of the National Criminal Police and RIA led to the identification of the Tallin resident. "During the searches, investigators found the downloaded photos from a database in the person's possession, along with the names and personal identification codes of the people," Oskar Gross, head of the police's cybercrime unit, said. Read the rest of the story by Pierluigi Paganini here: Security Affairs



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

Ransomware Case Study

By now, most of you have experienced some sort of a computer virus or malware attack either on your PC, your mobile phone or Tablet (Not talking about work or company computer here). Although in the majority of these cases, it was probably more than a time-consuming nuisance with minor financial outlay if you needed to pay the neighbours' kid to clean it out. Ransomware on the other hand is on a whole different playing field. In recent times we saw almost weekly reports of companies or big conglomerates that are hit by ransomware with sometimes astronomical amounts of money (or Bitcoins) demanded from the hackers to release a decryption key. Recently, however, we saw a new trend where more and more individuals are targeted with ransomware. These attacks are commonly earmarked as a so-called double hit where data is not only encrypted but copied too. Hackers are taking their time to gather tons of personal information on their victims and can easily determine if there are data bits that the individual would pay for to keep secret. Anyway, many have asked me for some case studies to help in their efforts to protect themselves. Unfortunately, I could not find a case study where an individual was targeted. Below however is a case study by Alissa Irei of TechTarget that would give you some insight into the pain and aftermath of a ransomware attack.

Ransomware attack case study: Recovery can be painful

Even with full backups and no permanent data loss, recovering from ransomware can be expensive and painful, as evidenced in this ransomware attack case study.

Ransomware case study: Attack #1

Several years ago, seasoned IT consultant David Macias visited a new client's website and watched in horror as it started automatically downloading ransomware before his eyes. He quickly unplugged his computer from the rest of the network, but not before the malware had encrypted 3 TB of data in a matter of seconds.

"I just couldn't believe it," said Macias, president and owner of ITRMS, a managed service provider in Riverside, Calif. "I'm an IT person, and I am [incredibly careful] about my security. I thought, 'How can this be happening to me?' I wasn't online gambling or shopping or going to any of the places you typically find this kind of stuff. I was just going to a website to help out a client, and bingo -- I got hit."

Macias received a message from the hackers demanding $800 in exchange for his data. "I told them they could go fly a kite," he said. He wiped his hard drive, performed a clean install and restored everything from backup. "I didn't lose anything other than about five days of work."

Ransomware case study: Attack #2

A few years later, in 2017, another of Macias' clients -- the owner of a direct-mail printing service -- called to report he couldn't access his server. Macias logged into the network through a remote desktop and saw someone had broken through the firewall. "I told the client, 'Run as fast as you can and unplug all the computers in the network,'" he said. This short-circuited the attack, but the hacker still managed to encrypt the server, five out of 15 workstations and the local backup.

"What made this ransomware attack so bad was that it attacked the private partition that lets you restore the operating system," Macias added. Although the ransom demanded was again only $800, he advised against paying, since attackers often leave backdoors in a network and can return to steal data or demand more money.

Fortunately, Macias had a full image-based backup of the client's network saved to a cloud service. Even so, recovery was expensive, tedious and time-consuming. He had to reformat the hard drive manually, rebuild the server from scratch and reinstall every single network device. The process took about a week and a half and cost $15,000. "The client was just incredibly grateful that all their data was intact," Macias said.

Although pleased the client's data loss was negligible, Macias wanted to find a more efficient, less painful disaster recovery strategy. Shortly after the second ransomware incident, he learned about a company called NeuShield, which promised one-click backup restoration. He bought the technology for his own network and also sold it to the client that had been attacked. According to NeuShield, its Data Sentinel technology works by showing an attacker a mirror image of a computer's data, thus protecting the original files and maintaining access to them even if encryption takes place.

Ransomware case study: Attack #3

In 2019, two years after the printing service's first ransomware incident, the company owner was working from home and using a remote desktop without a VPN. A hacker gained entry through TCP port 3389 and deployed ransomware, encrypting critical data. But Macias said NeuShield enabled him to restore the system with a click and reboot. "When they got hit the first time, it took forever to restore. The second time, they were back up and running in a manner of minutes," he said.

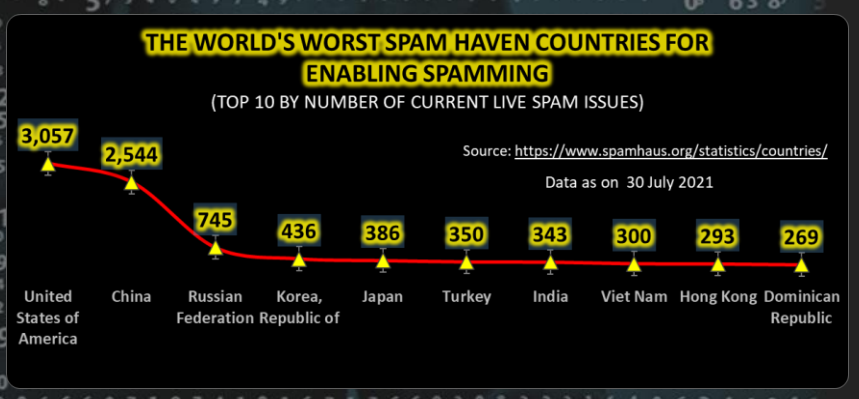
But while he sings NeuShield's praises, Macias noted the technology doesn't negate the need for antivirus protection to guard against common malware threats, or cloud backup in case of fires, earthquakes or other disasters. "Unfortunately, there's no one-stop solution," he said. "I wish there was one product that included everything, but there isn't."

Macias said he knows from personal experience, however, that investing upfront can prevent massive losses down the road. "I've had clients tell me, 'I'll worry about it when it happens.' But that's like driving without insurance. Once you get into an accident, it's too late."

(If you were the victim of a ransomware attack, please reach out to me, it would be great to share a real story as a case study)

Other Interesting News and Cyber Security bits:

- Four Ways Quantum Computing Could Change The World
- All EU member states commit to build a quantum communication infrastructure
- The quantum Internet: a glimpse at the future of connectivity



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