On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded).
Last Advisory 17 Jun 2021
Multiple Vulnerabilities in Apple iOS Could Allow for Arbitrary Code Execution.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
18 June	178,201,262	3,857,872

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
18 June 2021

In The News This Week

More than 1 Billion CVS Health records exposed in online database

Security researchers earlier this spring discovered a database containing more than a billion records, including emails that could be targeted in a phishing attack for social engineering. The database, which was not password-protected, was flagged by the WebsitePlanet research team in cooperation with Jeremiah Fowler. Public access to the data was restricted the same day that CVS Health was notified.
"In March of this year, a security researcher notified us of a publicly accessible database that contained non-identifiable CVS Health metadata," said CVS Health in a statement sent to Healthcare IT News. "We immediately investigated and determined that the database, which was hosted by a third-party vendor, did not contain any personally identifiable information of our customers, members or patients," according to the statement. "We've addressed the issue with the vendor to prevent a recurrence and we thank the researcher who notified us about this matter." Read the full story here: Healthcare IT News

Millions of Connected Cameras Open to Eavesdropping

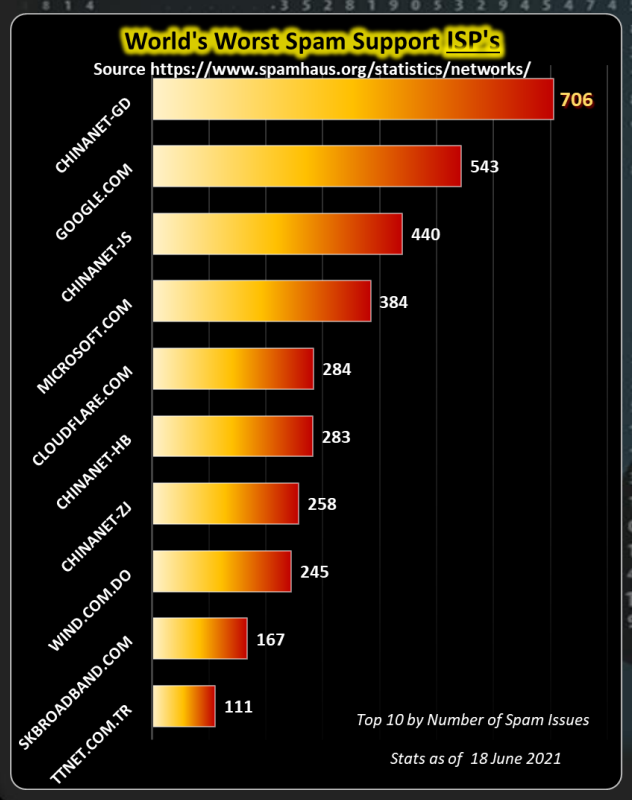
A supply-chain component lays open camera feeds to remote attackers thanks to a critical security vulnerability. Millions of connected security and home cameras contain a critical software vulnerability that can allow remote attackers to tap into video feeds, according to a warning from the Cybersecurity and Infrastructure Security Agency (CISA). The bug (CVE-2021-32934, with a CVSS v3 base score of 9.1) has been introduced via a supply-chain component from ThroughTek that's used by several original equipment manufacturers (OEMs) of security cameras – along with makers of IoT devices like baby- and pet-monitoring cameras, and robotic and battery devices. The potential issues stemming from unauthorized viewing of feeds from these devices are myriad: For critical infrastructure operators and enterprises, video-feed interceptions could reveal sensitive business data, production/competitive secrets, information on floorplans for use in physical attacks, and employee information. And for home users, the privacy implications are obvious. Read the story by Tara Seals here: ThreatPost

Russian National, Oleg Koshkin, Convicted of Charges Relating to Kelihos Botnet

A federal jury in Connecticut convicted a Russian national on Tuesday for operating a "crypting" service used to conceal "Kelihos" malware from antivirus software, enabling hackers to systematically infect victim computers around the world with malicious software, including ransomware. According to court documents and evidence introduced at trial, Oleg Koshkin, 41, formerly of Estonia, operated the websites "Crypt4U.com," "fud.bz" and others. The websites promised to render malicious software fully undetectable by nearly every major provider of antivirus software. Koshkin and his co-conspirators claimed that their services could be used for malware such as botnets, remote-access trojans, keyloggers, credential stealers and cryptocurrency miners. Koshkin was arrested in California in September 2019 and has been detained since his arrest. He faces a maximum penalty of 15 years in prison and is scheduled to be sentenced on Sept. 20. Read the full article here: US Dept. of Justice

Cruise operator Carnival discloses its third data breach since 2019

The world's largest cruise operator Carnival Corp. & plc today disclosed a new data breach involving the theft of personal data, its third data breach in just over two years. The latest data breach was detected on March 19. The breach involved the theft of "personal information relating to some guests, employees and crew for Carnival Cruise Line, Holland America Line, Princess Cruises and medical operations." The stolen data included names, addresses, phone numbers, passport numbers, dates of birth, health information — including COVID-19 testing — and in some cases, Social Security and national identification numbers. The exact form of the attack is not clear, with the company describing it as "unauthorized third-party access to a limited number of email accounts."
Carnival says it acted quickly to shut down the event to prevent further unauthorized access. The company added that they had engaged a leading cybersecurity firm to investigate the matter and have notified appropriate regulators. Read the full story by Duncan Riley here: SiliconAngle



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

Space Cybersecurity: How Lessons Learned on Earth Apply in Orbit

In my constant quest to research and share interesting cybersecurity bits, I often come across articles that really sparks my interest as it touches on both Cybersecurity and things I personally find fascinating. Two of these topics are space travel and quantum technology. Today I want to share a recent article by George Platsis of Security Intelligence dealing with Cybersecurity in Space. Below is a short extract of the article but please visit their website to read the full story if you find it as interesting as I do.

The universe is getting smaller, and space cybersecurity is keeping up. On May 30, 2020, nearly a decade after the Space Shuttle program ended, people witnessed a first: a vehicle built as part of a public-private partnership (between SpaceX and NASA) took off into space. This development was transformational because it brought the world one step closer to commercial space travel. We now have proof of concept that space travel, once reserved for powerful nation-states, is something that can be achieved, albeit with a lot of assistance right now, by a commercial company.
How safe space travel may be for everyday people is yet to be seen, but it's an exciting time because we can actually start talking space travel, space tourism and space mining.
But space travel is not cheap, and safety is not a joke. The risks that come with space travel mean you do not play games when it comes to redundant and backup options. When making these huge investments, you cannot afford to go bust or risk lives. That means as people make efforts to go more often and deeper into outer space, cybersecurity becomes a real issue that must be addressed.
Why? Well, think "E.T. phone home" as a start. If you want space travel safety, you have to be able to communicate.

Space and Cybersecurity - On Sept. 4, 2020, the White House issued the Memorandum on Space Policy Directive-5 — Cybersecurity Principles for Space Systems. Section 4, Principles is a worthwhile read for cybersecurity experts. Here is a brief overview of that section:

- Space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering.
- Owners and operators should develop and implement cybersecurity plans for their space systems.
- Protect against unwanted access to critical space vehicle functions.
- Include physical protection measures designed to reduce the risks of a space vehicle's command, control and telemetry receiver systems.
- Protect against communications jamming and spoofing.
- Protect ground systems, operational systems and data processing systems.
- Adopt appropriate cybersecurity hygiene practices, physical security for automated information systems and intrusion detection methodologies for system elements.
- Manage supply chain risks that affect the cybersecurity of space systems through tracking manufactured products.
- Space system owners and operators should collaborate to promote the development of best practices.
- Security measures should be designed to be effective while permitting space system owners and operators to manage risk tolerances and minimize undue burden. These must be consistent with specific mission requirements, United States national security and national critical functions, space vehicle size, mission duration, maneuverability and any applicable orbital regimes.

For any cybersecurity policy wonk, this is pretty much a dream-come-true list of security principles. But, don't we try to apply those same principles down here on planet Terra? Yes, we do. Emphasis on the word try.

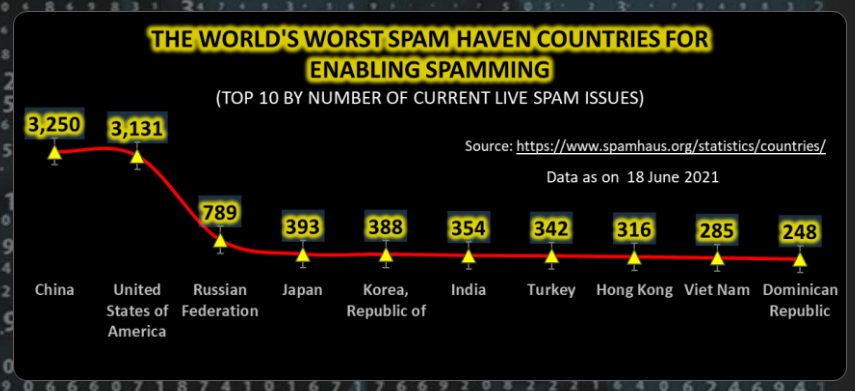
Today's World is Guided by Space Research - Unlike the internet, which is inherently vulnerable by design, there is an opportunity in space to build a uniquely secure means of communication that could not only reduce the dangers of research, but also could alter even land-based communications and way of life. For example, Space Policy Directive-5 gives us plenty of examples of how space research helps with homeland security.

Building Trustworthy Space Cybersecurity Systems - If you haven't heard of security-by-design, think about it like this. In its crudest form, it means to break while you build so you can fix and strengthen the weak spots. If you do this correctly and go above and beyond, you not only strengthen your system, you also build antifragility into your system. Nassim Nicholas Taleb, who coined the term antifragile, says this means the project doesn't merely withstand a shock, but improves because of it.
That's the chance we have with space systems that we don't have with the internet. In fact, the internet is the exact opposite of being antifragile because we keep building on its inherent risks, making it more complex and, in turn, more fragile.

Security for Telecommunications Networks at the Speed of Light - Let's take a look at a specific type of project that illustrates the way space cybersecurity professionals can apply to projects on Earth. Here on the ground, we're getting all excited about 5G, as we should be. But something else exciting is happening when it comes to satellite security: **quantum communications**. Leaving aside for a moment that we are still early into quantum communications development, or more accurately, quantum key distribution (QKD), QKD in theory, at least in space, should be easier to achieve. QKD is great when it comes to encryption because a user can identify right away if a message has been tampered with. In theory, QKD is unbreakable, because subatomic particles (photons) act in a very peculiar way. Mess with those particles and the message is no longer secure. That's awesome, right? How come we don't use QKD all the time? …. Read the rest of the article here: Security Intelligence

Other Interesting News and Cyber Security bits:

- Major Scientific Leap: Quantum Microscope Created That Can See the Impossible
- US Computer Fraud and Abuse Act: What the 'landmark' Van Buren ruling means for security researchers
- Hackers steals EA game source code and tools



Thank you to my good friend Yazan Shapsugh for his constant support and news contributions

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