On November 16, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Citrix, Apple, and Mozilla products.
CIS Security Advisories

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 November 2022

In The News This Week

China-Based Billbug APT Infiltrates Certificate Authority

Access to digital certificates would allow the Chinese-speaking espionage group to sign its custom malware and skate by security scanners. - The state-sponsored cyberattack group known as Billbug managed to compromise a digital certificate authority (CA) as part of a wide-ranging espionage campaign that stretched back to March — a concerning development in the advanced persistent threat (APT) playbook, researchers warn. Digital certificates are files that are used to sign software as valid and verify the identity of a device or user to enable encrypted connections. As such, a CA compromise could lead to a legion of stealthy follow-on attacks. "The targeting of a certificate authority is notable, as if the attackers were able to successfully compromise it to access certificates, they could potentially use them to sign malware with a valid certificate, and help it avoid detection on victim machines," according to a report this week from Symantec. "It could also potentially use compromised certificates to intercept HTTPS traffic.". Read the rest of the article by Tara Seals: Dark Reading

Netflix Phishing Emails Surge 78%

Security researchers are warning that corporate accounts could be at risk after noting a 78% increase in email impersonation attacks spoofing the Netflix brand since October. If employees use the same credentials for personal accounts like Netflix as their work accounts, campaigns like this may imperil corporate systems and data, warned Egress. The group behind this particular campaign is using Unicode characters to bypass natural language processing (NLP) scanning in traditional anti-phishing filters, the security vendor claimed. "Unicode helps to convert international languages within browsers – but it can also be used for visual spoofing by exploiting international language characters to make a fake URL look legitimate," Egress wrote. "For example, you could register a phishing domain as 'xn–pple-43d.com,' which would be translated by a browser to 'apple.com.' This is known as a homograph attack." Unicode is also used in the sender display names, such as "Netflix" and "help desk." However, the threat actors didn't stop there.... Read the rest of the story by Phil Muncaster here: InfoSecuritly

Researchers Discover Hundreds of Amazon RDS Instances Leaking Users' Personal Data

Hundreds of databases on Amazon Relational Database Service (Amazon RDS) are exposing personal identifiable information (PII), new findings from Mitiga, a cloud incident response company, show. "Leaking PII in this manner provides a potential treasure trove for threat actors – either during the reconnaissance phase of the cyber kill chain or extortionware/ransomware campaigns," researchers Ariel Szarf, Doron Karmi, and Lionel Saposnik said in a report shared with The Hacker News. This includes names, email addresses, phone numbers, dates of birth, marital status, car rental information, and even company logins. Amazon RDS is a web service that makes it possible to set up relational databases in the Amazon Web Services (AWS) cloud. It offers support for different database engines such as MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server.
The root cause of the leaks stems from a feature called public RDS snapshots, which allows for creating a backup of the entire database environment running in the cloud and can be accessed by all AWS accounts.
Read the full story by Ravie Lakshmanan here: The Hacker News

Iranian Hackers Compromised a U.S. Federal Agency's Network Using Log4Shell Exploit

Iranian government-sponsored threat actors have been blamed for compromising a U.S. federal agency by taking advantage of the Log4Shell vulnerability in an unpatched VMware Horizon server. The details, which were shared by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), come in response to incident response efforts undertaken by the authority from mid-June through mid-July 2022. "Cyber threat actors exploited the Log4Shell vulnerability in an unpatched VMware Horizon server, installed XMRig crypto mining software, moved laterally to the domain controller (DC), compromised credentials, and then implanted Ngrok reverse proxies on several hosts to maintain persistence," CISA noted...
Read the story by Ravie Lakshmanan here: The Hacker News

A new cyber taskforce will supposedly 'hack the hackers' behind the Medibank breach. It could put a target on Australia's back

- The Australian government is launching an offensive against cybercriminals, following a data breach that has exposed millions of people's personal information. On November 12, Minister for Cyber Security Clare O'Neil announced a taskforce to "hack the hackers" behind the recent Medibank data breach. The taskforce will be a first-of-its-kind permanent, joint collaboration between Australian Federal Police and the Australian Signals Directorate. Its 100 or so operatives will use the same cyber weapons and tactics as cybercriminals use, to hunt them down and eliminate them as a threat. Details on how the taskforce will operate remain murky, partly because it needs to keep this information away from criminals. But the fact remains that taking an offensive stance, while it could deter further attacks, could also put a big red cross on Australia's back. Read the full article and watch the video clip of MP Clare O'Neil here: The Conversation

The Electric Power Grid and Cyber Security

The continual war and attack on the Ukrainian infrastructure highlighted one of the most critical components of our global supply chain, the electric power grid, and its sub-components. In our modern era, power generation and distribution became highly digitized. With interconnected IT and OT networks and computer systems to manage it all, Cyber Risk is now greater than ever before. This is evident as we've seen in recent times how a Cyber Attack left Ukraine without power for hours. This was done by successfully unleashing malware that has been around for some years called "Industroyer". Another recent attack on Ukraine's energy grid was successfully thwarted, but this time the culprit was "Industroyer2", a spruced-up version of the original. These attacks are only examples of many more attacks on critical infrastructure across the world, and according to experts, the onslaught has just begun. It was a hot topic on the recent SMART GRID FORUMS - IEC 61850 Week 2022 event held in October in Cardiff United Kingdom, and I came across a comprehensive summary of the event by Dr. Jesus Molina of Waterfall that I would like to share today. Please find an extract of Dr. Molina's overview below.

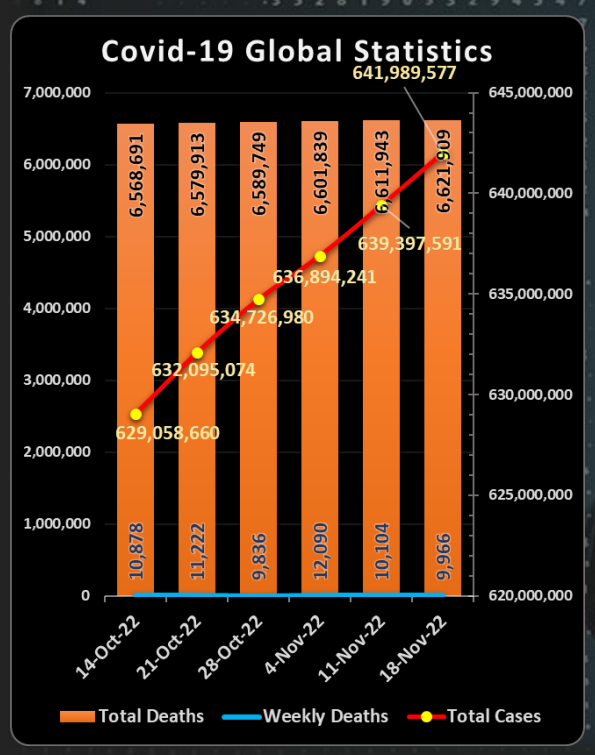
Waterfall - Our summary of the Power Grid Cyber Security at the IEC 61850 Smart Grid Conference

Reframing the Wild Cyber "*GOOSE*" Chase with Sensible Segmentation

A cornerstone of our critical energy infrastructure is the electric power grid, a network of transmission lines and substations that crisscross the globe. Of the two, perhaps substations stand as the most complex and fragile element. Making substations more efficient is increasingly necessary, as an expanding grid requires an enhanced substation infrastructure based on digitization. Ultimately, resiliency and efficiency are not possible to achieve without power grid cyber security. Many elements interface here, including SCADA systems, critical infrastructure, and suitability of the IEC 62443 standard. What's most important, however, is how this all boils down to the IEC 61850 standards
In a recent conference of the commanding standard available on the segment, IEC 61850 Week by Smart Grid Forums, the best and the brightest of the industry came together to evaluate the implementation of the standard and the novelties of its implementation. There was no shortage of questions after every talk. Virtualization at the substation was a big topic, but the spotlight was on the use and improvements of GOOSE (Generic Object-Oriented Substation Event).
GOOSE is a communication model defined by the IEC 61850 standard, which uses fast and reliable mechanisms to group any format of data (status, values) and transmit it across communication networks within 4 milliseconds. This is most used to connect between substation IED (Intelligent Electronic Devices), which is great, as it allows not only efficient communication but also reliability and interoperability between vendors. To communicate between TSO (Transmit System Operators), IEC61850 also defines the MMS protocol, that uses a client server model, and can be routed over the internet.

At the conference, Waterfall Security participated in a panel alongside DNV and Rheebo. Rheebo opened the discussion with Intrusion Detection Systems and their role in substations. DNV provided useful information on the utilization of IEC 62351, the current standard for security in energy management systems and associated data exchange. Waterfall discussed the raise of attacks with physical consequences, and the role of unidirectional gateway technologies in a defense in depth architecture required by TSOs. The topic of power grid cyber security appeared in many talks apart from the panel, mainly as part of methods to create encryption envelopes for GOOSE packets to route them as R-GOOSE, or as part of particular use cases such as remote access.

I Felt a Strange Déjà Vu From Three Years Ago - Back then I participated in a rail signaling systems conference, and all looked too familiar. Expert engineers discussing how to improve a real-time system, that was safety critical and used protocols that had no authentication nor encryption. While peppering their talks with some cyber security 101, they were noting that nothing could be done in the short term. In fact, due to the very work they were doing on standardizing the communication, this will allow an attacker to simply understand the protocol to create a destructive payload in a much shorter time frame.
Before I continue, let me bring up one important fact: Industroyer, the malware that left Ukraine without power for hours, and Industroyer2, the enhanced malware that recently attempted and narrowly failed this year, ***both include IEC 61850 destructive payloads***.
In the case of signaling systems, the industry acted, and TS-50701 was born. It requires strong segmentation for safety critical segments, including the substations, as they are essential parts of the rail network that electrify the train. Figure 1 is the example included in TS-50701 on how to segment rail power networks. In this example, the substation is in SL-5 (Safety) connecting to the Control Center, also SL-5 (Safety). Connecting safety networks to external networks requires Unidirectional Technologies or a very well managed – and probably expensive – DMZ .
But during the conference, segmentation was an afterthought and that was bothersome, given that we are talking about the power grid cyber security, a critical infrastructure . The problem here is GOOSE not only makes life simpler for the IED manufacturers, but also for an attacker to launch orchestrated attacks. R-GOOSE allows for the attacks to spread between substations. This is because, in most implementations, GOOSE is a multicast protocol with no authentication or encryption. And let me repeat, IEC 61850 has already been weaponized by nation state malware. (e.g. – Diagram- Industrial network plant energy)
The following week after I attended the Smart Grid Conference, I attended the EUTC and EE-ISAC event at the European Parliament. The most enlightening part of the event was of course over drinks. I was still rummaging about what happened at the event the previous week when I started a chat with Stephan Lechner. He discussed an article he authored (link) on reviewing the cyber security strategies for the European grid. In that review, three elements stood out: (1) The real-time performance requirements of the power grid do not allow for overhead, so standard cyber security elements such as authentication are not readily available. (2) the impact of successful attacks may create a cascading failure effect. (3) Existing, legacy systems need to interact with new devices, increasing the risk of cyber attack
All of this applies directly to what I learnt the previous week! GOOSE is a real-time protocol, that in most implementations lacks security. R-GOOSE allows for interconnecting substations, thus increasing the risk of cascading effects. Techniques, such as virtualizing substation IEDs, merges legacy systems with very capable datacenters, which are much more susceptible to attacks as they use commercial off-the-shelf software.... That is all I have space for in this post folks, please see the full article by Dr. Molina here: Waterfall Security

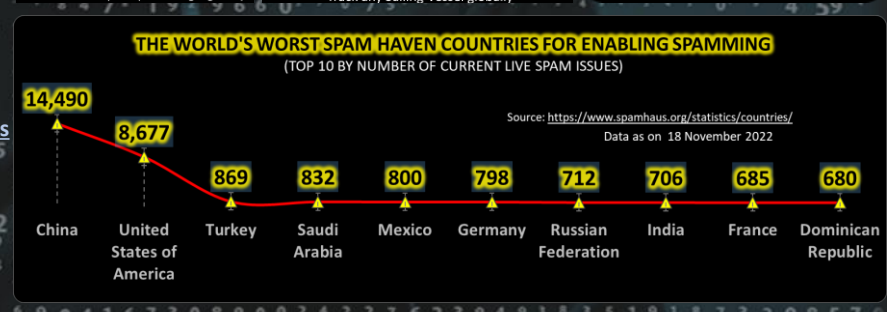


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Other Interesting News and Cyber Security bits:

- Lift off! NASA finally launches Artemis rocket ship for voyage to the moon
- NASA's James Webb spots galaxies formed mere 35 crore years after the Big Bang
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
Marine Traffic Track any Sailing Vessel globally
SatelliteXplorer Track satellites in orbit



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