On August 9, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Microsoft, and Adobe 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
11 August 2023

In The News This Week

New 'Downfall' Flaw Exposes Valuable Data in Generations of Intel Chips

The vulnerability could allow attackers to take advantage of an information leak to steal sensitive details like private messages, passwords, and encryption keys. - INTEL IS RELEASING fixes for a processor vulnerability that affects many models of its chips going back to 2015, including some that are currently sold, the company revealed today. The flaw does not impact Intel's latest processor generations. The vulnerability could be exploited to circumvent barriers meant to keep data isolated, and therefore private, on a system. This could allow attackers to grab valuable and sensitive data from victims, including financial details, emails, and messages, but also passwords and encryption keys. Read the rest by Lily Hay Newman here: Wired

North Korean hackers breached top Russian missile maker

An elite group of North Korean hackers secretly breached computer networks at a major Russian missile developer for at least five months last year, according to technical evidence reviewed by Reuters and analysis by security researchers. Reuters found cyber-espionage teams linked to the North Korean government, which security researchers call ScarCruft and Lazarus, secretly installed stealthy digital backdoors into systems at NPO Mashinostroyeniya, a rocket design bureau based in Reutov, a small town on the outskirts of Moscow. Reuters could not determine whether any data was taken during the intrusion or what information may have been viewed. In the months following the digital break-in Pyongyang announced several developments in its banned ballistic missile programme but it is not clear if this was related to the breach. Read the full article here: Reuters

Northern Ireland police data breach is second in weeks, force reveals

Admission that document with names of 200 staff was stolen in July follows revelation of 'monumental' data breach on Tuesday. - The Police Service of Northern Ireland has admitted that this week's "monumental" data breach followed an earlier leak of names of hundreds of officers and staff, deepening a crisis over the mishandling of personal information that could be used to target employees. The disclosures sowed anxiety in the ranks and prompted some officers to relocate in case paramilitaries tried to exploit the situation – the terrorism threat level in the region is categorised as severe, meaning the chances of an attack are deemed highly likely. Read the rest of the article here: The Guardian

Panasonic Warns That IoT Malware Attack Cycles Are Accelerating

Devices for the Internet of Things has been plagued for more than a decade by security issues and unresolved vulnerabilities that fuel botnets, facilitate government surveillance, and expose institutional networks and individual users around the world. But many manufacturers have been slow to improve their practices and invest in raising the bar. At the Black Hat security conference in Las Vegas today, Panasonic researchers unveiled the company's strategy for enhancing IoT defences, based on a five-year project to collect and analyze data on how the company's own products are being attacked.
Read the full story by Zack Zwiezen here: US Times Post

TargetCompany Ransomware Deploy Fully Undetectable Malware on SQL Server

The TargetCompany ransomware (aka Mallox, Fargo, and Tohnichi) is actively targeting the organizations that are using or running vulnerable SQL servers. Apart from this, recently, the TargetCompany ransomware unveiled a new variant of malware along with several malicious tools for persistence and covert operations that are gaining traction rapidly. Cybersecurity researchers at Trend Micro discovered a recent active campaign linking Remcos RAT and TargetCompany ransomware and compared to past samples, the new deployments use fully undetectable packers.
Read the rest of the story by Divya here: GBHackers

Windows Defender-Pretender Attack Dismantles Flagship Microsoft EDR

A newly patched flaw in Windows Defender allows attackers to hijack the signature-update process to sneak in malware, delete benign files, and inflict mayhem on target systems. - BLACK HAT USA – Las Vegas – Wednesday, Aug. 9: Among the 97 CVEs that Microsoft patched in April 2023 was a security feature bypass vulnerability that allows an unprivileged user to hijack Windows Defender and use it to wreak havoc on target systems. Researchers at SafeBreach — who discovered similar vulnerabilities in security products previously — uncovered the issue with Windows Defender during an attempt take over the antivirus tool's update process. The research goal was to verify if the update process could be used to sneak known malware into systems the software is designed to protect. Researchers also wanted to verify if they could get Windows Defender to delete signatures of known threats and worse, to delete benign files and trigger a denial-of-service condition on a compromised system.. Read full story by Jai Vijayan here: Dark Reading

"Social Engineering" – Don't take the bait

I'm sure that most of you have been subjected to a barrage of cybersecurity awareness campaigns in your workplace, and you kind of get desensitized about the whole idea. That is, unfortunately, one of the dangers of overstating the mostly obvious threats we are facing on a daily basis, and your security department is just doing its job. The poor guys are dealing with users that clicked on a bad link or did something stupid on a daily basis, and they cannot understand why the awareness campaigns are failing, what more can they do?

Desensitizing someone towards a threat or adverse situation through overexposure or other techniques is a form of social engineering. Many years ago when I was a conscript in the army, I remember they deployed similar types of techniques to desensitize us for when we are in a battle situation in order to concentrate on the job at hand and not get caught up in what is happening around you. Techniques to train or untrain your psychic behaviour towards certain subjects or situations are indeed psychological engineering.

The cybercriminals of today, are highly aware of the psychological arena created where the "constant threat" versus the "constant awareness" battle is playing out. And, they know that social engineering still works as effectively as in the beginning.

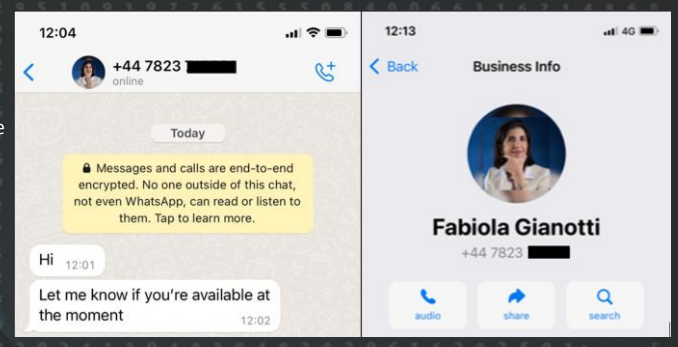
So, let's look at what social engineering is in the context of cybersecurity. I've done my usual walkabout in the Internet woods and found a few articles of which I will share some extracts. As usual, I'll place links to all the resources at the bottom of this post.

Social Engineering – "STOP – THINK"

"Social engineering" is the art of manipulating you to perform actions you would not normally perform. Like transferring money to someone you don't know ("LOGISTICS SUPPORT REQUEST"). Disclosing sensitive information ("I have problems displaying that doc"). Opening doors to an unknown third party ("I forgot my access card"). Or handing out your CERN password, e.g. during our annual clicking campaigns ("Action Required – Warning!!") intended to raise security awareness.

In order to achieve their goals, attackers try to forge a close connection with you. "Greetings to you and your family. How are you doing?" is still a very basic try, but given the information that can be found online about you, your family and social circle, your work and your hobbies, social engineers might delve much, much deeper. Just think of the information available about you on Facebook, Instagram, LinkedIn and CERN's many webpages ("The symbiosis of your life"). How easily can your life be reconstructed from that information? (Here and here are two nice videos about this topic.) How much "juicy" stuff is out there to allow them to connect with you, build up a trust relationship and lure you into actions you wouldn't normally perform for a stranger? This social engineering is a long process, but an attacker is ready to go the distance if the outcome – i.e. you disclosing sensitive information, handing over your password or transferring money – is worth it. Think about your role in this Organization: there is definitely something worth attacking you for. Access to accelerator controls to conduct sabotage if you work in the accelerator sector; access to money or personal information if you work in finance and administration; or access to computing services, data and databases if you are an IT administrator.

The picture on the right shows an attempt to connect with some of CERN's colleagues, in this case using WhatsApp:

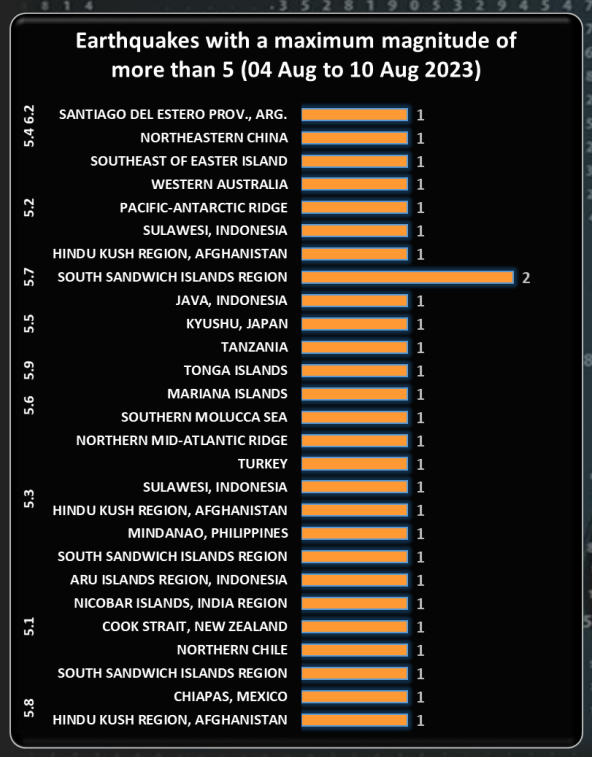


It wouldn't be the first time that the Director-General's authority has been abused for social engineering purposes. And it won't be the last. Here, we can't tell how that conversation would have continued, but usually it leads to a demand for a money transfer ("CEO fraud").
So, be vigilant if you are contacted by people you don't know or receive requests that are unusual, from unsolicited contacts.
Be careful if you are asked to perform tasks you usually only perform in the execution of your job but never on direct request.
"STOP – THINK – DON'T CLICK" when you get a link in an email, text message, WhatsApp message or through a QR code. And, maybe, rethink the plethora of information you voluntarily make public via your social channels – check your privacy and publication settings! – or on CERN webpages. Maybe a bit less information would do your privacy good and protect you a bit more from social engineering?

Social Engineering – some real life examples

1. **Persuasive email phishing attack imitates US Department of Labor** - In January 2022, Bleeping Computer described a sophisticated phishing attack designed to steal Office 365 credentials in which the attackers imitated the US Department of Labor (DoL).
2. **Deepfake Attack on UK Energy Company** - In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring $243,000 to a "Hungarian supplier" — a bank account that actually belonged to a scammer.
3. $60 Million CEO Fraud Lands CEO In Court - Chinese plane parts manufacturer FACC lost nearly $60 million in a so-called "CEO fraud scam" where scammers impersonated high-level executives and tricked employees into transferring funds. After the incident, FACC then spent more money trying to sue its CEO and finance chief, alleging that they had failed to implement adequate internal security controls.

Resources: CERN, Tessian



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:

- DARPA Launches AI Cyber Challenge to Drive Innovation in Cybersecurity
- How Can Passengers' Personal Devices Potentially Pose Cyber Threats To Aircraft?
- Who's Hacked? Latest Data Breaches And Cyberattacks (Cybercrime Magazine)
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit

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