On April 6, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Zyxel, Trend Micro, Apple, Google, and Mozilla products.
CIS 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

08 April 2022

In The News This Week

FBI Cybersecurity Strike Against Russian Botnet Is 'Awesome Moment' For MSPs

The FBI's successful pre-emptive strike that stopped a Russian-government-backed botnet aimed at taking down SMB and home-office networks is a landmark moment in the battle to protect Main Street from foreign cybersecurity attacks, said MSPs. "This is an awesome moment for MSPs," said David Stinner, president of Buffalo, N.Y.-based MSP US itek, reacting to the FBI operation. "The U.S. government just launched a pre-emptive strike against Russian hackers that benefits MSPs everywhere. It is fantastic to know that the FBI is protecting us with this kind of cyber warfare. Kinetic war is the war of the past. Cyber warfare is the war of the future. I am ecstatic that we have the U.S. government protecting us from these kind of attacks.".. Read the full story here: CRN

Ukraine Warns of Cyber attack Aiming to Hack Users' Telegram Messenger Accounts

Ukraine's technical security and intelligence service is warning of a new wave of cyber attacks that are aimed at gaining access to users' Telegram accounts. "The criminals sent messages with malicious links to the Telegram website in order to gain unauthorized access to the records, including the possibility to transfer a one-time code from SMS," the State Service of Special Communication and Information Protection (SSSCIP) of Ukraine said in an alert. The attacks, which have been attributed to a threat cluster called "UAC-0094," originate with Telegram messages alerting recipients that a login had been detected from a new device located in Russia and urging the users to confirm their accounts by clicking on a link. Read the story by Ravie Lakshmanan here: TheHackerNews

Anonymous allegedly gained access to the Kremlin's CCTV system

"Now we're inside the castle, Kremlin." - After Russia's invasion of Ukraine started on February 24, the global hacker group Anonymous waged a cyberwar aimed at sabotaging President Vladimir Putin's government. Now, an unconfirmed report alleges that Anonymous gained access to the Russian government's CCTV cameras. In a tweet posted on Wednesday, April 6, AnonymousTV states that "hackers (@Thblckrbbtworld) who operate [on] behalf of #Anonymous gained access to the Kremlin CCTV system." The user quotes the Anonymous group as saying, "we won't stop until we reveal all of your secrets. You won't be able to stop us. "Now we're inside the castle, Kremlin." Alongside the post is a video — yet to be independently verified — of surveillance footage showing Russian officials from their own CCTV cameras. Read the rest of the story here: Interesting Engineering

Anonymous hacker collective leaks one million Kremlin emails in massive attack on Putin

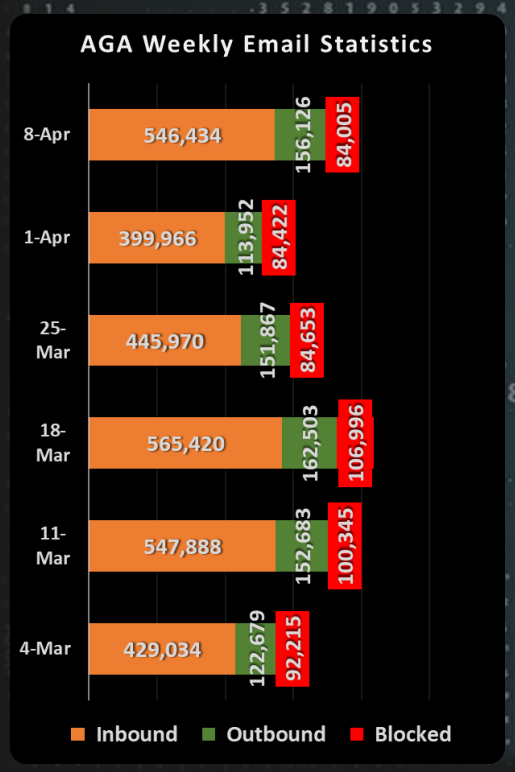
The hacker collective Anonymous claims to have seized around 900,000 emails from deep within the Russian government, in what is perhaps the biggest cyber attack on the Kremlin during Russia's Ukraine offensive yet. The leaked emails have allegedly been taken from Russia's biggest state media network which has been repeatedly accused of spreading propaganda during the conflict. Anonymous has made public hundreds of thousands of emails from the All- Russia State Television and Radio Broadcasting Company (VGTRK), which operates five TV stations in Russia. Emma Best, Co-founder DDoSecrets, tweeted: "#DDoSecrets has received the VGTRK (All-Russia State Television and Radio Broadcasting Company) data and will release it in the near future. "Transparency is coming to Russia, one leak at a time. Read the story in British papers here: Daily Star, DailyMail

Anonymous takes revenge on Putin's brutal Ukraine invasion by leaking personal data of 120,000 Russian soldiers

- Hacker collective Anonymous announced on Twitter that it successfully breached and leaked the personal data of 120,000 Russian soldiers. "All soldiers participating in the invasion of Ukraine should be subjected to a war crime tribunal," Anonymous said in the message. The leak included personal information like dates of birth, addresses, passport numbers, and unit affiliation. Read the story here: Fortune

Microsoft Obtains Court Order to Take Down Domains Used to Target Ukraine

Microsoft on Thursday disclosed that it obtained a court order to take control of seven domains used by APT28, a state-sponsored group operated by Russia's military intelligence service, with the goal of neutralizing its attacks on Ukraine. "We have since re-directed these domains to a sinkhole controlled by Microsoft, enabling us to mitigate Strontium's current use of these domains and enable victim notifications," Tom Burt, Microsoft's corporate vice president of customer security and trust, said. APT28, also known by the names Sofacy, Sednit, Pawn Storm, Fancy Bear, Iron Twilight, and Strontium, is a cyber espionage group and an advanced persistent threat that's known to be active since 2009... Read the story here: The Hacker News



For Reporting Cyber Crime in South Africa go to **Alert Africa** or **Cybercrime**
For the USA, go to the Internet Crime Compliant Center (IC3) **www.ic3.gov**

What Is the Metaverse, Exactly?

The latest buzzword flying around is the "Metaverse", particularly after Facebook rebranded itself as "Meta" to embrace this concept. Curiosity then got the better of me and I wanted to know what this means exactly and why the big hype?
As I was traversing around in cyberland, I came across this article by Eric Ravencraft from Wired that sort of gives you an idea of the concept. Below then is an extract of Eric's article.

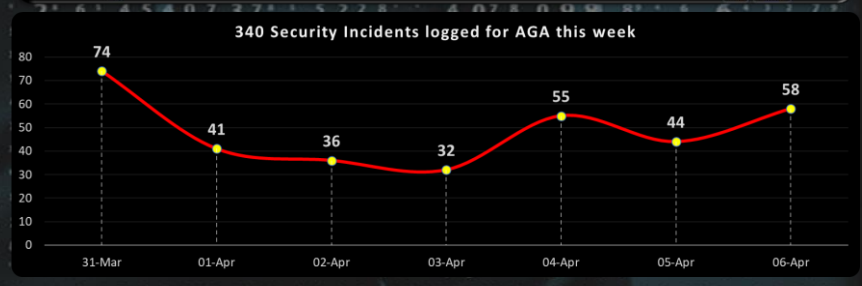
What Is the Metaverse, Exactly?

To hear Tech CEOs like Mark Zuckerberg or Satya Nadella talk about it, the metaverse is the future of the internet. Or it's a video game. Or maybe it's a deeply uncomfortable, worse version of Zoom? It's hard to say.
To a certain extent, talking about what "the metaverse" means is a bit like having a discussion about what "the internet" means in the 1970s. The building blocks of a new form of communication were in the process of being built, but no one could really know what the reality would look like. So while it was true, at the time, that "the internet" was coming, not every idea of what that would look like is true. On the other hand, there's also a lot of marketing hype wrapped up in this idea of the metaverse. Facebook, in particular, is in an especially vulnerable place after Apple's move to limit ad tracking hit the company's bottom line. It's impossible to separate Facebook's vision of a future where everyone has a digital wardrobe to swipe through from the fact that Facebook really wants to make money selling virtual clothes… So, with all that in mind …
Seriously, What Does 'Metaverse' Mean? - To help you get a sense of how vague and complex a term "the metaverse" can be, here's an exercise to try: Mentally replace the phrase "the metaverse" in a sentence with "cyberspace." Ninety percent of the time, the meaning won't substantially change. That's because the term doesn't really refer to any one specific type of technology, but rather a broad shift in how we interact with technology. And it's entirely possible that the term itself will eventually become just as antiquated, even as the specific technology it once described becomes commonplace.
Broadly speaking, the technologies that make up the metaverse can include virtual reality—characterized by persistent virtual worlds that continue to exist even when you're not playing—as well as augmented reality that combines aspects of the digital and physical worlds. However, it doesn't require that those spaces be exclusively accessed via VR or AR. A virtual world, like aspects of Fortnite that can be accessed through PCs, game consoles, and even phones, could be metaversal.
It also translates to a digital economy, where users can create, buy, and sell goods. And, in the more idealistic visions of the metaverse, it's interoperable, allowing you to take virtual items like clothes or cars from one platform to another. In the real world, you can buy a shirt from the mall and then wear it to a movie theatre. Right now, most platforms have virtual identities, avatars, and inventories that are tied to just one platform, but a metaverse might allow you to create a persona that you can take everywhere as easily as you can copy your profile picture from one social network to another.
It's difficult to parse what all this means because when you hear descriptions like those above, an understandable response is, "Wait, doesn't that exist already?" World of Warcraft, for example, is a persistent virtual world where players can buy and sell goods. Fortnite has virtual experiences like concerts and an exhibit where Rick Sanchez can learn about MLK Jr. You can strap on an Oculus headset and be in your own personal virtual home. Is that really what "the metaverse" means? Just some new kinds of video games?
Well, yes and no. Saying that Fortnite is "the metaverse" would be a bit like saying Google is "the internet." Even if you could, theoretically, spend large chunks of time in Fortnite, socializing, buying things, learning, and playing games, that doesn't necessarily mean that it encompasses the entire scope of the metaverse.
On the other hand, just as it would be accurate to say that Google builds parts of the internet—from physical data centers to security layers—it's similarly accurate to say that Fortnite creator Epic Games is building parts of the metaverse. And it isn't the only company doing so. Some of that work will be done by tech giants like Microsoft and Facebook—the latter of which recently rebranded to Meta to reflect this work, though we're still not quite used to the name. Many other assorted companies—including Nvidia, Unity, Roblox, and even Snap—are all working on building the infrastructure that might become the metaverse.
It's at this point that most discussions of what the metaverse entails start to stall. We have a vague sense of what things currently exist that we could kind of call the metaverse, and we know which companies are investing in the idea, but we still don't know what it is. Facebook—sorry, Meta, still not getting it—thinks it will include fake houses you can invite all your friends to hang out in. Microsoft seems to think it could involve virtual meeting rooms to train new hires or chat with your remote co-workers.
The pitches for these visions of the future range from optimistic to outright fan fiction. At one point during … Meta's … presentation on the metaverse, the company showed a scenario in which a young woman is sitting on her couch scrolling through Instagram when she sees a video a friend posted of a concert that's happening halfway across the world.
The video then cuts to the concert, where the woman appears in an Avengers-style hologram. She's able to make eye contact with her friend who is physically there, they're both able to hear the concert, and they can see floating text hovering above the stage. This seems cool, but it's not really advertising a real product, or even a possible future one. In fact, it brings us to the biggest problem with "the metaverse."
Why Does the Metaverse Involve Holograms? - When the internet first arrived, it started with a series of technological innovations, like the ability to let computers talk to each other over great distances or the ability to hyperlink from one web page to another. These technical features were the building blocks that were then used to make the abstract structures we know the internet for: websites, apps, social networks, and everything else that relies on those core elements. And that's to say nothing of the convergence of the interface innovations that aren't strictly part of the internet but are still necessary to make it work, such as displays, keyboards, mice, and touchscreens….

This is unfortunately all I have space for in this post, but if I triggered your curiosity, please read the rest of Eric's article here: Wired

Other Interesting News and Cyber Security bits:

- Cloud 'data bursts' from space move astronauts closer to Mars — and improve life on Earth
- Shore thing: climate change and maritime security intrinsically linked
- Microsoft security chief warns of metaverse crime
- SANS Daily Network Security Podcast (Storm cast)



Author: Chris Bester - Please feel free to contact the Security team for any security issue - Cyber.Alerts@anglogoldashanti.com