2022/04/15

Security topics 03

So that critical infrastructures can be operated all the time🥺 (04/14/2022)

I was reading ZDNet's article called "These ten hacking groups have been targeting critical infrastructure and energy". Thank you very much.😊 In this article, based on a report released by Dragos, a cybersecurity company, it explained that critical infrastructures vital to our everyday lives such as electricity, oil, and gas are exposed to the risk of cyberattacks, and it's introducing 10 hacking groups. The following are quotes from this article:

> The list includes several state-backed hacking operations, such as **Electrum – also known as Sandworm – which is linked to the Russian military**, Covellite, which is linked to North Korea's Lazarus Group, and Vanadinite, which is lined to APT 41, a hacking operation working on behalf of China.

> As more critical infrastructure is connected to the internet or accessible to staff by remote desktop protocols and VPNs, it's increasingly becoming a target for nation-state backed hackers and cyber criminal gangs interested in breaching and examining OT networks to lay the groundwork for future campaigns.

OT: operational technology

> **After hackers enter industrial networks, it's unlikely to have an immediate impact on the systems controlling operational processes because it could take years for attackers to understand everything – but it's about laying the foundations for this for the future**.

> The campaigns being tracked by Dragos have a variety of aims - some are around stealing information, or there could potentially be plans to cause disruption – for example, cyber criminals looking to launch ransomware attacks. **The nature of operational technology and a reliance on older software and protocols means any evidence of compromise can be missed, proving hackers with ample time to move around, understand and gain control of networks**.

> It's this what researchers describe as "the biggest cybersecurity weakness" facing industrial networks, because without having a full picture of what needs to be protected from cyber attacks, it's not possible to fully defend networks from hackers.

> The also paper warns that activity related to cyber attacks targeting industrial infrastructure has been observed since Russia's invasion of Ukraine and western cybersecurity agencies have issued warnings on the need to protect networks from attacks.

> In addition to having a good understanding of what's on the network, many standard cybersecurity practices can help secure OT networks. **These include applying security updates to patch known vulnerabilities in software, and**

> **applying multi-factor authentication whenever possible**.

I thought we had to think about critical infrastructures we are using.🥺 I think it's necessary not only to have these companies strengthen their security so that these services can be operated all the time, but also think about when it comes to stopping these services by hackers. If not, in the end, we will get in trouble.🥺

I'd like to add information about Electrum (aka Sandworm) especially.😃The following is a quote from this article:

> Electrum: this group is capable of developing malware that can modify and control OT procedures and Dragos researchers say this operation was responsible for Crash Override – also known as **Industroyer** – a malware attack on Ukraine's power grid in December 2016. Electrum is associated with Sandworm, an offensive hacking operation that's part of Russia's GRU military intelligence agency.

And thanks to Catalin Cimpanu's retweet, I was able to know about SSSCIP Ukraine's tweets. Thank you very much.😊 Recently, there is information that **Industroyer2 malware was used for substations in Ukraine**. In ESET's report, it is said that it is the new version of Industroyer. The following are quotes from this tweet:

> @_CERT_UA under the @dsszzi reported a #Sandworm (UAC-0082) #cyberattack on Ukraine’s energy infrastructure

> suing #Industroyer2 and #CaddyWiper malware.
> The attackers attempted to take down several infrastructure components of their target, namely: (1/5) #CyberWar #WARINUKRAINE

> **Electrical substations — using #Industroyer2 malware**.
> Every executable file contained a statically configured set of unique parameters for one of the target substations. (2/5)

> Windows-operated computing systems (user computers, servers, APCS workstations) — using #CaddyWiper destructive data wiper.
> Linux-operated server equipment — using malicious destructor scripts.
> Active network equipment (3/5)

> As reported, the target organization suffered two attack waves. The initial compromise occurred not later than in February 2022. And on Friday evening, April 8, the attackers planned shutting down the electrical substations and taking down the enterprise's infrastructure (4/5)

> However, the malicious intent has been prevented
> To determine whether there is a similar threat for other Ukrainian organizations, the information, including malicious software samples, has been shared with the international partners and #Ukraine's energy sector enterprises (5/5)

It's amazing that the Ukrainian government's computer emergency response team (CERT-UA) and ESET were able to deal with it well.👏Will Japanese power companies's substations be okay? 🥺

Also, thanks to Catalin Cimpanu's Retweet and Dr. Dan Lomas' tweet, I was able to know about a factsheet of the British government on cyber operations and intelligence agencies in Russia. Thank you very much.😊The following are quotes from this factsheet:

> **Cyber operations against worldwide critical national infrastructure**
> Centre 16 of the FSB have targeted/gained unauthorised access systems in countries around the world that are necessary for a country to function and upon which daily life depends. Known as Critical National Infrastructure or CNI, Centre 16 has targeted systems essential for energy, healthcare, finance, education and local/national governments. This has been a concerted campaign over many years and in a wide range of countries across Europe, the Americas and Asia.

> NCSC and cyber security companies have warned network defenders on multiple occasions of the risks posed by this pattern of activity. While there has been speculation of FSB involvement, the UK government is confirming this activity was carried out by FSB Centre 16 and providing further details of specific examples of this activity to increase awareness and transparency around the threat.

This factsheet introduced cases of cyber operations in Russia subsequent to the above description. 😀

I was also able to find out in the latest episode of the Wired UK podcast that the Ukrainian subway station functions as a bomb shelter. Thank you very much.😊I've found a video

related to this called "Ukraine Civilians Use Subway Station As Bomb Shelter Amid Russian Invasion". Thank you very much.😊

As it was introduced in this episode, Arsenalna station was the deepest subway station in the world.😳😳

I was also reading an article called "The Deepest Metro Stations in The World". Thank you very much.😊The following is a quote from this article:

> Arsenalna station is located 105.5 meters below the surface, making it the deepest metro station in the world. If you made a vertical shaft on earth as deep, you could drop the entire Statue of Liberty into it and still have more than twelve meters of headroom left to drop other stuff. To board a subway train at this station, commuters have to take two seemingly never-ending escalators to the bottom. The journey takes up to five minutes.

Image： the escalator at Arsenalna metro station from its Ukrainian wiki

page

Keywords: Critical Infrastructure, Dragos, Electrum, Industroyer, Industroyer2, State Service of Special Communications and Information Protection of Ukraine, ESET, FSB Centre 16, Bomb shelter, Arsenalna station

A power of administrator privileges is scary in a way🥺 (03/28/2022)

I was listening to the latest episode of the podcast Wired UK. One story was that the U.S. telecommunications company Viasat caused disrupted broadband satellite Internet access in Ukraine coinciding with Russia's invasion. Thank you very much.😊Also, I was able to know the story from Runa Sandvik's tweet via Matthew Green's retweet before. Thank you very much.😊There was an introduction to a Reuters article in that tweet. Below are quotes from this article:

> The consequences are still being investigated but satellite modems belonging to tens of thousands of customers in Europe were knocked offline, according to an official of U.S. telecommunications firm Viasat, which owns the affected network.

> The hackers disabled modems that communicate with Viasat Inc's KA-SAT satellite, which supplies internet access to some customers in Europe, including Ukraine. More than two weeks later some remain offline, resellers told Reuters.

> Government contracts reviewed by Reuters show that KA-SAT has provided internet connectivity to Ukrainian military and police units.

> Pablo Breuer, a former technologist for U.S. special operations command, or SOCOM, said knocking out satellite internet connectivity could handicap Ukraine’s ability to combat Russian forces.

> The Viasat official said a misconfiguration in the "management section" of the satellite network had allowed the hackers remote access into the modems, knocking them offline. He said most of the affected devices would need to be reprogrammed either by a technician on site or at a repair depot and that some would have to be swapped out.

According to the story of Wired UK, this seems that disabled modems are occurring even a month after in France, Germany, the United Kingdom, Poland and Morocco. I've learned that if administrators don't prevent mistakes in setting up a "management section" to manage the network, it will cause tremendous damage in some cases.🧐

Keywords: Satellite Internet Access, Modem, KA-SAT, Satellite, Hacker, Russia, Ukraine