Cyberwatch Finland

WEEKLY REVIEW WEEK 2/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. Nuclear power plants are an attractive target for both cybercriminals and nation-state supported hacker groups.

2. The number of cyberattacks on Australia has been on the rise. There are both economic and geopolitical reasons behind this.

3. Malvertising's popularity as a tool for cyberattackers has risen. In certain respects, it may be more effective than traditional phishing.

1. CYBER RISKS OF NUCLEAR POWER

The safety of nuclear power plants has always been a hot topic. Recently, attention has been focused on cyber threats to them. Although nuclear power plants are not on the list of the most attacked targets, they are definitely not completely free of the threat. Most recently, there were examples of this in the UK, when the media reported on two cases of cyber influencing on a nuclear power related organisation. One of these came last week, when Radioactive Waste Management, a British public organisation focusing on nuclear waste management, announced that it had been the target of targeted and long-running phishing attempts. The incident itself was not serious and, according to the organization itself, the attacks were unsuccessful, but it illustrates the interest towards the field. The significance is increased by the fact that this has been apparently planned and targeted specifically at this organisation.

The second case relates directly to the nuclear power plant rather than to the treatment of nuclear waste. In December 2023, the British newspaper The Guardian reported that it had learned that the systems of one of the country's most important nuclear power plants, Sellafield, had been hacked years ago. Reportedly, it is likely that not all remnants of the malware have been removed and the plant's management has even tried to cover it up. According to anonymous sources, information about hackers' access to the plant's systems and sensitive data has been known, but very little has been done about it. In general, there have allegedly been many significant shortcomings in the plant's cyber security culture. Although anonymous journalism should be treated with caution, the fact that last week the chief cyber security officer responsible for cyber security at this plant announced his resignation and responsibility for cyber security has been transferred to a different executive.

In both cases, the motives behind the action are unclear. According to sources, both Chinese and Russian hackers have been involved in the Sellafield case, but there is no further information about the attackers' goals, at least not publicly. On one hand, it would be even quite worrying if high-risk targets had only been hit by a financially motivated operator who is not aware of or simply does not care about the risk that disruption of nuclear power plants may cause. One the other hand however, it is perhaps more likely that behind the attacks exists a conscious and intended influence on specifically nuclear power plants by a nation-state directed hacker group. Power plants are attractive targets in many ways. While financially motivated crime would be attracted solely by the criticality of the industry and thus a higher probability of, for example, paying ransoms, state influence is also attracted by the significance of the activities to national energy production and, for example, the significant information value associated with successful attacks. In Finland, for example, outages in nuclear power plants receive wide attention, regardless of the reason causing them. The rise in electricity prices caused by outages is almost immediately felt in the everyday lives of ordinary citizens as well. The informational effect of a cyberattack on a nuclear power plant is also significant. In Britain, the debate on the safety of nuclear power has increased significantly in recent months, although the attacks did have not at least yet caused obvious or severe harm.

If the phenomenon is examined historically, it is clear that cyber influencing of nuclear power plants is not necessarily shy away. Over the past year, Russia, in particular, has demonstrated, in the form of military action against the Zaporizhzhia nuclear power plant, that it is prepared to use nuclear risks as a negotiating tool. The best-known cyberattack against nuclear power is also one of the most well-known cyberattacks in general and considered the best example of long-term high-level state cyber influencing. It is more than a decade old Stuxnet malware that targeted Iranian uranium enrichment plants and was likely a fact-finding and sabotage operation carried out jointly by the United States and Israel.

There is considerable interest and threats to nuclear power and nuclear power plants in the cyber environment. Like any other industry, the nuclear power industry has become significantly digitalized in recent years. Expanded production networks and value chains, as well as remote control of old devices not intended to be connected to the network, have significantly increased the threat area. The cyber security of nuclear power has generally been considered good, and the plants are certainly among the organisations most seriously responding to security threats. On the other hand, news such as Sellafield is shaky, because with high interest, even the slightest laxity in security can lead to the realization of threats. The amount of interest should be taken into account not only in the activities of the operators themselves, but also in the activities of all subcontractors related to nuclear power production, especially as the impact on critical infrastructure and the energy economy is expected to continue to grow.

2. AUSTRALIAN CYBER THREAT LANDSCAPE

At the turn of the year, there were reports from Australia of several cyberattacks targeting the country. In December, attacks included Eagers Automotive, the country's largest car dealership, and Victoria's state legal services, which fell victim to ransomware. Earlier in November, the country's ports were targeted in a cyberattack on DP World Australia, which disrupted the handling of more than 30,000 shipping containers in five different ports. According to a report published a year ago by technology company BlackBerry, Australia is one of the countries facing the most cyberattacks in the world, ranking fifth in terms of the number of cyberattacks. The trend of cyberattacks is also growing. In its November report, the Australian Signals Directorate ASD, which is responsible for the security of the country's networks and communications, said cyberattacks had increased by almost a quarter from a year ago. What explains Australia's attractiveness as a target for cyberattacks and how is the country prepared for the threat?

Simply put, Australia's appeal as a target for hackers is influenced by both economic and geopolitical reasons. Australia is a developed and economically strong state. According to the International Monetary Fund, the country ranks 12th in terms of GDP per capita. This makes the country an attractive target for financially motivated cybercriminals. Naturally, attacks are targeted at actors who are thought to be able to afford to pay, for example, ransom demands for ransomware. The economic consequences can be significant. An Australian police spokesman estimated in December that ransomware has a negative impact of up to 3 billion Australian dollars annually on the country's economy. Russian-backed ransomware gangs in particular have excelled in attacks.

Some attacks, on the other hand, take place for purely geopolitical reasons. At the moment, the threat comes particularly from China. For example, the aforementioned ASD highlighted Chinese state-sponsored hackers as a major player in cyberattacks against large corporations and critical infrastructure. Australia has traditionally been a close ally of the United States and is a party to the 2021 AUKUS military cooperation agreement with the United Kingdom and the United States, which is de facto aimed to deter against Chinese influence. China and Australia can therefore be seen as competitors in the Asia-Pacific region. This has also been reflected in the trade war between the two countries, in which Australia denied Chinese Huawei the right to participate in the construction of the country's 5G network. China has responded with its own sanctions, although it has eased them somewhat during 2023. In addition to China, other state actors have also shown interest in Australia. For example, Iranian actors are known to have carried out cyberattacks.

Although Australia faces a lot of cyberattacks and has been in the headlines, the country has historically been considered as a country with high level of cybersecurity. This may also partly explain the high number of cyberattacks – they are detected and reported openly. The country has prepared for the ransomware threat on a long-term basis. Back in 2021, the then Australian government published a Ransomware Action Plan (RAP) aimed at fighting the threat. In addition, the high level of cyber security is affected by, among other things, the high-quality education opportunities available in the country and international cooperation, which has been carried out, for example, within the framework of the above-mentioned AUKUS cooperation and the Five Eyes intelligence cooperation. The country has also developed its offensive cyber capacity and allocated more funds for cybersecurity. The latest example is the government's new seven-year cyber strategy, published at the end of November, which aims to make Australia a world leader in cybersecurity. In practice, this means financial investments in cyber security and additional funding of AUD$586.9 million to achieve the targets. The money is intended to support small and medium-sized enterprises, raise awareness of cyber threats and fight cybercrime, among other things. The funding comes on top of the $2.3 billion in investments already approved. Both financial investments and extensive international cooperation indicate that cyber security is being taken seriously. In the end, however, the focus will be on how well the cyber-secure culture can be implemented in the daily operations of Australian companies and organisations. Financial investments give a head start, but do not solve problems if the implementation is not completed.

Cyberwatch Finland

3. MALVERTISING IS BECOMING MORE COMMON

It is difficult to avoid annoying and intrusive advertising on the Internet. Ads can be found on social media platforms, website sidebars and search engine results. As digital platforms grow in popularity, so do the number of ads. In addition to being annoying, online ads can pose a real threat because they can be driven by cybercriminals trying to deceive. Malvertising, a combination of malware and advertising, has been developed to describe criminal activity that uses advertising or advertisements to distribute harmful content. In practice, malvertising refers to any activity in which a threat actor hides harmful content inside an ad. The term can be used to describe, for example, a method in which cybercriminals use a credible-looking advertisement to trick potential victims into clicking on a link to a scam website. Clicking on a malicious ad can directly trigger malware downloads and also lead to a data-stealing website. At worst, just watching an ad can trigger malicious content to load.

The harmfulness of online ads or the risks associated with clicking on them have been talked about for years. It's good to note that malicious ads don't just appear in untrustworthy corners of the web or stand out clearly from legitimate, completely harmless ads. Malvertising has made a rise in the popularity of cybercriminal tools and it has also developed to be harder to detect. Especially over the past year, there have been several cases where advertisements containing malware had been used in large-scale cybercrime operations instead of more traditional phishing. The latest example came in mid-December when security company Mandiant published a report on a previously unknown threat actor it tracked and named UNC2975. For several years, the threat actor had successfully injected malware into thousands of devices almost exclusively using advertisements. In particular, the hacker group had taken advantage of purchased advertising space from various search engines on the web, which is quite a popular and effective method of malvertising.

Search engines such as Google or Bing (both of which UNC2975 had also used in its operations) are widely abused in distributing malicious advertisements. While most malicious content is detected before it reaches the ads that users see, some malicious content always gets through the net. Naturally, search engines try to prevent the spread of malware on their platforms and avoid situations where links containing

malicious content rise to the top of search results. However, control is often passive. Accurate analysis only occurs if users report a particular ad enough times, or if automated analytics detects something suspicious enough in the ad or website. Scammers often know how to avoid this surveillance. They also have ways to hide malicious content from both automatic scanning and a quick glance by the victim. Often, the same scams don't stay visible long enough for the number of reports to reach a significant level. Even if the site manually removes the ad from viewing, the loss to the criminal is not great. From the criminal's point of view, the operation is relatively risk-free and easy. Credible scam content or advertisements are easy to make, and ready-made templates are cheaply available on the black market. In addition, the risk of getting caught is quite small. Often, disclosure only leads to interruption of activities, and only extremely rarely do those who engage in malverting actually be held accountable.

Malvertising has been estimated to be more effective in some cases than more traditional phishing or sending scam messages directly to victims. People often have healthy reservations about contacts from unknown sources. Although phishing is still the most popular and effective form of attack, threat awareness has increased. It is more difficult to detect malicious content in the feed of search engines. Links that result from a self-entered search and appear identical to those that have been clicked on before may seem trustworthy. In other words, the user "finds" the malicious content themselves, and no one tries to feed it to them, which means that the protective walls may be lower. The ever-increasing number of AI-based search engines adds to the threat. Last year, there was a lot of talk about how people trust too much in the answers produced by artificial intelligence. The answers they provide are not sufficiently questioned or the sources are not verified independently. It is hardly surprising that efforts have also been made, and succeeded, in infiltrating the input of AI search engines. For example, in late autumn 2023, Microsoft's Bing Chat search engine was found to make an ad-boosted scam site the only result for certain searches and in some cases, a scam site that mimicked the original would rank higher in search results than the genuine page.

Thus, advertisements are not harmless, and they are widely used in various cyberattacks. Naturally, they are less effective than targeted phishing, for example, in operations targeting a specific actor, but they make it possible to reach large numbers of potential victims with less risk. Protecting yourself from malvertising, like other common cyber scams, is easy in principle, but often very difficult in practice. The instructions are often repeated and known to everyone, but they cannot be overemphasized. Links should always be checked beforehand before clicking, no links or advertisements should be clicked "just to see", organizations should emphasize staff training on proper online activities, and caution should also be exercised when using routine web applications or search engines. A threat can never be eliminated, but awareness of it and sharing information are the best ways to minimize the risk.

REFERENCES

1. Cyber risks of Nuclear Power

Computer and information security at nuclear facilities | IAEA
Sellafield nuclear site hacked by groups linked to Russia and China | Energy industry | The Guardian
UK nuclear waste firm thwarts cyberattack | SC Media (scmagazine.com)
Sellafield's longest serving director to step down - GOV.UK (www.gov.uk)
Stuxnet explained: The first known cyberweapon | CSO Online
What to do about the Zaporizhzhia nuclear power plant | Brookings

2. Australian Cyber Threat Landscape

https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative/
https://therecord.media/hackers-breach-australian-court-hearing-database
https://www.abc.net.au/news/2023-11-15/asd-reports-increase-in-cyber-attacks/103103320
https://www.abc.net.au/news/2024-01-06/ransomware-attacks-court-systems-australia/103287138
https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook47p/ThreatRansomware
https://www.bleepingcomputer.com/news/security/dp-world-confirms-data-stolen-in-cyberattack-no-ransomware-used/#google_vignette
https://www.canberratimes.com.au/story/8466144/fbi-decryption-key-frees-australian-businesses-from-blackcat-ransomware/
https://www.imf.org/external/datamapper/NGDPDPC@WEO/OEMDC/ADVEC/WEOWORLD/AUS
https://www.politico.com/news/2021/09/15/biden-deal-uk-australia-defense-tech-sharing-511877
https://www.reuters.com/legal/litigation/australias-eagers-automotive-says-it-systems-hit-by-cyber-incident-2023-12-28/
https://www.reuters.com/technology/australia-inc-roiled-by-raft-cyberattacks-this-year-2022-11-07/
https://www.reuters.com/technology/cybersecurity/australia-goes-cyber-offensive-with-sweeping-resilience-plan-2023-11-22/
https://www.reuters.com/technology/cybersecurity/australia-says-state-sponsored-cyber-groups-targeting-critical-infrastructure-2023-11-15/

3. Malvertising is Becoming More Common

Opening a Can of Whoop Ads: Detecting and Disrupting a Malvertising Campaign Distributing Backdoors | Mandiant
The forgotten malvertising campaign (malwarebytes.com)
Malicious ad served inside Bing's AI chatbot (malwarebytes.com)
AI Chatbots Are Coming to Search Engines. Can You Trust Them? | Scientific American
Malvertising Is Once Again on the Rise Leading to Malware Infections - CyberHoot

Pictures: Pixabay