SECTRA NEWSLETTER – June 2024

Monthly Review

Cybersecurity news from around the world

ARTICLE

Log data as a target and tool for cyberattacks

Read article →

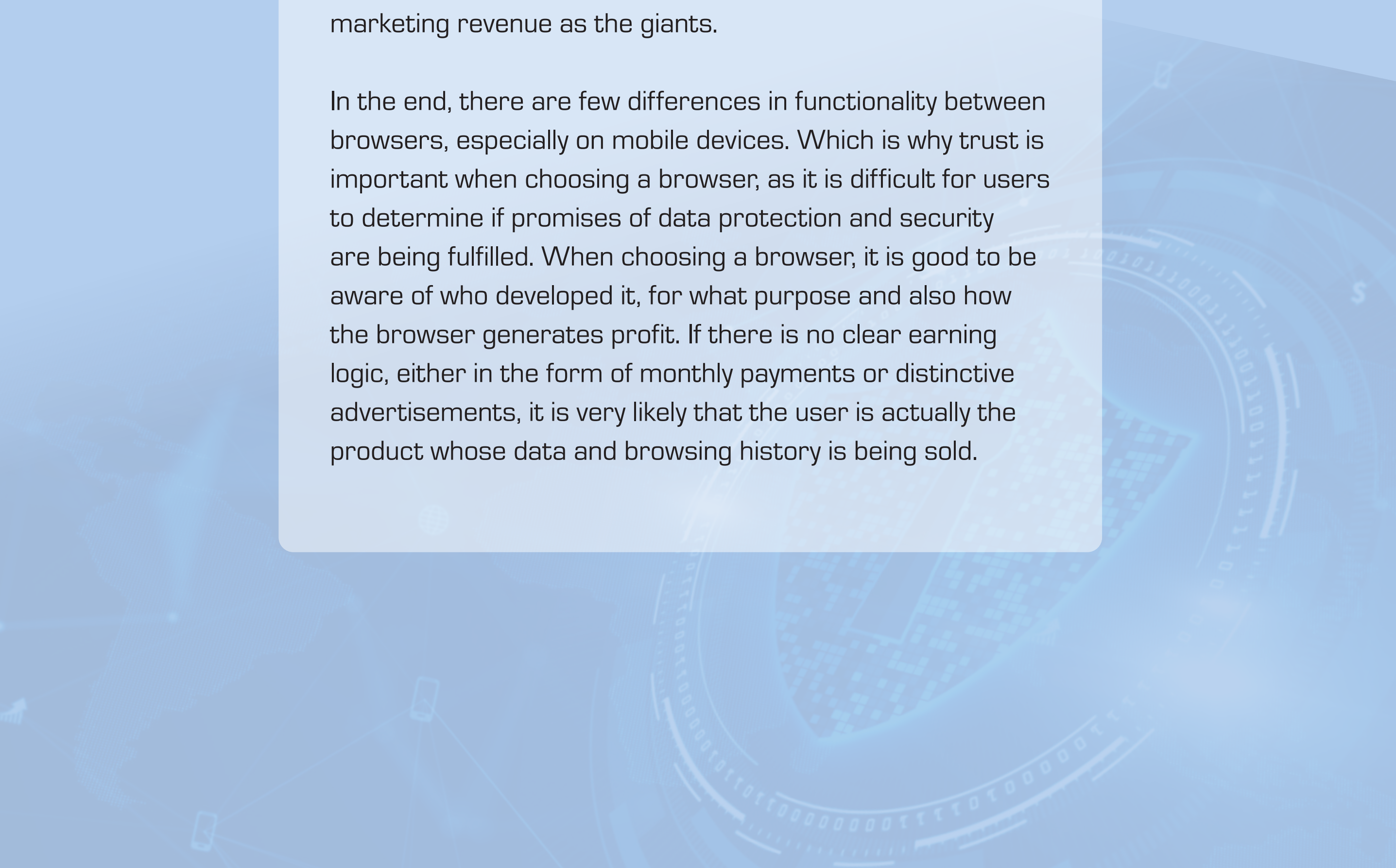
SECTRA

General cybersecurity news

1 Small browser manufacturers market themselves with privacy

The EU's Digital Markets Act (DMA) has begun to disrupt the monopoly of data giants in the digital market. The regulation has created more equal competition for small companies developing alternatives to dominant digital products. Companies like Apple and Google are now required to allow the use and marketing of applications, browsers, and app stores other than their own. Since the regulation came into effect, there has been an increase in the popularity of smaller browsers, although the market is still largely dominated by the giants. The main differentiator among browsers is the level of privacy they offer, with some smaller browsers emphasizing privacy as a selling point. However, these smaller platforms do not generate the same scale of marketing revenue as the giants.

In the end, there are few differences in functionality between browsers, especially on mobile devices. Which is why trust is important when choosing a browser, as it is difficult for users to determine if promises of data protection and security are being fulfilled. When choosing a browser, it is good to be aware of who developed it, for what purpose and also how the browser generates profit. If there is no clear earning logic, either in the form of monthly payments or distinctive advertisements, it is very likely that the user is actually the product whose data and browsing history is being sold.



2 Healthcare sector targeted by cybercriminals

Cyber threats to healthcare have been highlighted globally during spring 2024. News of attacks come in on almost weekly basis. Most recently in May news about a ransomware attack on Scotland's public health service gained a lot of attention. Another major attack has been a ransomware attack on US-based United HealthCare. The attack caused widespread disruption and eventually forced the company to pay a ransom to the criminals. Still, not all systems and functions could be restored. While attacks are often motivated by financial gain, there are concerns of political or hybrid influencing objectives as well. To mitigate risks, healthcare organizations should prioritize staff training, raise awareness, and implement technical measures such as hardware upgrades and network segmentation.

3 Paying ransom is tempting, but never useful

Ransomware attacks continue to pose a significant threat in the cybersecurity landscape. These attacks can be initiated through various means, such as infected email attachments, advertisements, or malware embedded in links or websites. Once a computer is infected, access to the device or its files is locked. Some attackers also engage in data breaches, where sensitive information is stolen and held for ransom. Despite the staggering amount of ransom payments, experts and authorities insist that paying the ransom is not the right course of action. Recent cases have highlighted the futility of paying ransoms. In one instance, a Chinese online store paid a ransom to the attacker who hijacked its database, only to face further extortion demands. Another case involved a healthcare company in the United States paying a ransom, but the attacker vanished with the money, leaving the door open for further blackmail. Paying the ransom does not guarantee data recovery and only perpetuates the cycle of crime, making the victim more vulnerable to future attacks.

ARTICLE

Cyber threats to the Olympics

There is an increased risk of cyber threat activity towards the Paris Olympics. This includes cyber espionage, disruptive and destructive operations, financially motivated criminal activity, hacktivism, and various information operations.

These cyber threats can affect a variety of targets, including event organizers and sponsors, ticketing systems, Paris infrastructure, and athletes and spectators travelling to the event. In addition, they can also influence the audience following the Olympics globally through the media. Russian state-sponsored groups are currently the biggest risk in cyberspace ahead of the Paris Olympics. In addition to espionage campaigns, Russian actors have already demonstrated their ability and willingness to carry out destructive campaigns, both in the information and cyber environment. France has been one of Europe's leading countries in providing financial and military support to Ukraine in the war against Russia and that continues to raise the risk of Russian cyber influence in France.

In concrete terms, these attacks are likely to appear as various information operations due to the huge global media coverage of the Olympics. These information operations can be misinformation and disinformation spread in various ways, and also DDoS attacks on systems, sites or transmissions are likely to happen. In addition to these, various wiper-attacks and attacks that otherwise disturb the harmony of the Olympic Games may be possible by Russian threat actors. →

Any successful attack on the Olympics has informational value. If cyber influencing succeeds in disrupting the Games, it will be a victory for Russia, as it shows France's lack of ability to organize secure Games and manage cybersecurity in a proper manner. This information effect is global, as the attention of the whole world is focused on an event lasting a few weeks. Russians have a lot of experience in disrupting the Olympic Games. Due to the current global political situation, more harassment and attempts to influence can be expected.

“Any successful attack on the Olympics has informational value.”

In addition to Russians, other actors also have the motivation to exploit visibility provided by the games with the aim of gaining reputation, financial profit or highlighting ideology or a political issue. APT groups supported by other states are also expected to take advantage of the summer Olympics through various operations. Cyber espionage campaigns are targeted especially at guests arriving at the games. The arrival of representatives of various governments and other decision-makers in Paris provides an excellent opportunity for many state actors to carry out their espionage and influence operations.

Financially motivated criminals are attracted by the economic circus created by the Olympic Games, which certainly opens up a wide range of possibilities for carrying out lucrative criminal activities. This activity can occur, for example, as spoofing various sites, services or products, i.e. creating scam sites that mimic real services. Through these, criminals let victims understand that they are dealing with a different entity or service than they think and try to get victims to enter valuable personal information into scam websites. →

Financially motivated criminals are very likely to use the Olympic theme to carry out various phishing or other scam campaigns. The purpose of these phishing scams is, for example, to impersonate various authorities or organizers, and to obtain personal data, online banking credentials and usernames for different platforms. Criminals can also carry out attacks directly on the organizer's information systems, allowing them to gain access to large amounts of critical information about the organizers of the Olympic Games, but also about guests and partners. This information benefits both cybercriminals and state APT actors, so attacks or attempted attacks directly on these systems are likely.

Preparing for Olympic cyber threats

The threat of cyber influencing of the Olympic Games has been known for a long time, and preparations have also been underway for years. The French authorities have developed new systems, intensified cooperation with private companies and tested the operation of new solutions in confined environments. The most important actor in cyber preparedness has been the French cybersecurity authority ANSSI (Agence nationale de la sécurité des systèmes d'information). Together with a few private companies they have prepared for the expected attacks, and especially the systems that have become operational in recent months have been stress-tested, both by flesh-and-blood hackers and by AI applications looking for vulnerabilities.

Being prepared involves communicating the threat and risk factors ahead of time and openly acknowledging the threat actors. By announcing in advance that prominent threat actors are likely to launch cyberattacks against the Games, the impact of these attacks can be reduced, even if they are successful. While this does not completely eliminate the informational value of a successful attack, early warning significantly affects how disturbances or faults are addressed. When Russia's motivations and likelihood of attempting to influence the event are announced well ahead of the Games, a successful attack will no longer come as much of a surprise and shock.

To stay safe online, it's important to know about potential cyber threats ahead of time. One common threat is spoofing, where attackers create fake websites that mimic legitimate ones. By being cautious and alert, it's possible to avoid falling for these tricks. When visiting Olympic-related sites or services, always double-check the URL to make sure it's correct and doesn't contain any suspicious or incorrect elements. Spoofed sites often use a similar URL to the real one, but with slight changes or incorrect language.

It's also worth noting that paid advertisements appear at the top of search engine results. This means that the genuine results for legitimate sites might be pushed down below these paid ads. Criminals often pay for these top positions to promote their spoofed sites. Organizations involved in the Games or sending employees to the event should inform and warn their staff about cyber threats in advance. Educating employees about different scams and cyber threats related to travel is a good idea. By practicing good cyber hygiene and staying aware, individuals can minimize their risks, especially considering the significant number of scam services that may be present during the Games. ■

ARTICLE

Log data as a target and tool for cyberattacks

The concept of log data revolves around the historical records generated by information devices and systems. These logs provide valuable information about the actions performed on a device or system, including when and by whom.

The primary purpose of log data is to investigate malfunctions and attacks, enabling organizations to gain insight into their IT infrastructure and the activities that have taken place within it. This includes details such as user activities, system searches, and communication patterns. Additionally, log data may contain internal and external contact information for the organization. Although log data itself may not be considered critical information, when combined with other data, it can play a crucial role in the success of future cyberattacks. Logs can unveil personally identifiable and regulated information, methods of obfuscating traces, and tactics used for harassment and extortion. Consequently, log data is highly sought after on the black market and is even used during the Resource Development phase of cyber attacks. According to MITRE ATT&CK®, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, the Resource Development phase means that the adversary is trying to establish resources they can use to support future operations. →

Attackers analyze log data to identify weaknesses in a system, potentially revealing behavioral or defense patterns. By gaining access to log data, an intruder also acquires additional useful information from the system, making it a secondary target rather than the primary one. Moreover, attackers may manipulate log data to camouflage their own activities and delay the defense's response. This confusion can hinder systems that monitor and alert against attacks and abuses.

Log data is of interest not only to financially motivated criminals but also to state-sponsored cyberspies. They can be used to carry out successful cyberattacks aimed at stealing or encrypting company confidential information. Additionally, it can be leveraged for long-term intelligence operations by cyberspies who have gained unauthorized access to systems.

> *“Log data is of interest not only to financially motivated criminals but also to state-sponsored cyberspies.”*

One notable example within recent years is the Log4j version 2 vulnerability, which exposed organizations worldwide to multiple exploits. Log4j is a widely used open-source log data framework, and the vulnerability allowed attackers to steal usernames and passwords, inject data, and introduce malware into systems. Reports indicate that globally, 2% of organizations will still be using that version of the vulnerability in 2024, despite a patch being released shortly after the discovery of the vulnerability in 2021. →

The primary threats surrounding log data lie in the security and monitoring of an organization's log management systems. It is crucial for organizations to ensure that their programs and log frameworks are regularly updated to protect against vulnerabilities. Neglecting these updates may make systems more vulnerable to various cyber attacks.

In summary, log data plays a significant role in cybersecurity investigations. Its analysis can uncover valuable insights into system activities and provide warnings of potential threats. It is vital for organizations to prioritize the security of their log management systems by ensuring their software and frameworks are up-to-date. By doing so, organizations can mitigate risks and bolster their defenses against potential cyber attacks. ■

Key takeaways

1. The EU's new Digital Markets Act has enabled smaller web browsers to compete with data giants.

2. The healthcare sector remains a top target for cyberattackers.

3. When facing blackmail, paying the ransom may seem tempting, but in reality, it rarely does anything but make things worse.

4. A wide variety of cyber influencing can be expected in the Olympics. Russian cyber threat actors are expected to be active perpetrators of attacks.

5. Logs are not usually considered as critical data, but they provide both an attractive target and a tool for cybercriminals..

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.

SECTRA