Monthly Review

Cybersecurity news from around the world

GENERAL CYBERSECURITY NEWS 2

ARTICLES

The threat posed by ransomware affects everyone 4

Exploitation of zero-day vulnerabilities on the rise 8

KEY TAKEAWAYS 11

ARTICLE

Exploitation of zero-day vulnerabilities on the rise

Read article →

SECTRA

General cybersecurity news

1 State-owned hacker group targets U.S. government

During April, the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. cyber and information security agency, issued a warning to government organizations about potential Russian cyber intruders. The warning is based on concerns that attackers may have managed to infiltrate systems by exploiting data stolen from Microsoft earlier this year. Microsoft announced in January that it had experienced a data breach in which an attacker gained access to emails from the U.S. government and Microsoft's own source code, among other things.

The hacker group known as Midnight Blizzard, Cozy Bear or APT29 was found to be behind the attack. This group is widely associated with the Russian Foreign Intelligence Agency (SVR) and is considered one of Russia's most powerful state-owned hacker groups. CISA urged all government organizations to inspect their systems for intrusion that has already occurred and to be cautious in the near future. It says it is likely that the hacker group is trying to continue its attack on some part of the government or an agency working for it. Neither Microsoft nor CISA has exactly disclosed what information Midnight Blizzard has obtained. CISA said the leaked data posed a "grave and unacceptable threat." The warning applies to all entities under the U.S. government.

2 Security risks of a public Wi-Fi

Using public Wi-Fi networks can pose security risks. Sensitive data can be intercepted by threat actors, and there are other information security risks as well. Network owners can view and intercept data traffic on public networks. Criminals can create fake networks to steal information. It's important to be cautious of the reliability and security of the network provider. Infected devices and hackers may also be present on public networks. To protect against these threats, it is best to avoid using public Wi-Fi or limit the use of sensitive information. Companies should provide guidelines on the use of public Wi-Fi on work computers. Using secure websites that encrypt communications and using VPNs are recommended methods to reduce risks.

3 Weak cybersecurity of small businesses

The UK published a report revealing that only about 22% of companies in the country have a cyber incident plan, with small companies being the least prepared. Similar studies suggest that small businesses globally are inadequately prepared and resilient to cyberattacks. While there is a misconception that small businesses face fewer cyber threats, they are actually attractive targets due to their vulnerability. Poor security levels, unsecured infrastructure, and lack of cyber hygiene make them easy targets. Evolving legislation and guidelines, such as the NIS2 Directive, emphasize the need for smaller companies to prioritize cyber risk management. Developing a situational understanding, maintaining up-to-date security measures, and increasing awareness among management and staff are crucial steps in enhancing cybersecurity. Investing in proactive cybersecurity measures is more cost-effective than dealing with the aftermath of an attack.

ARTICLE

The threat posed by ransomware affects everyone

Ransomware is a widespread cyber threat that affects organizations and individuals. It has targeted large companies such as Sony, Boeing, MGM Resorts, as well as public sector operators like universities and municipalities. Estimates suggest that criminals earned up to $1.1 billion from ransomware attacks in the previous year alone.

Ransomware works by locking, encrypting, or hijacking devices or files and demanding a ransom, usually in the form of bitcoins or another cryptocurrency, for their release. The device or data can be restored with an encryption key that the criminals promise to give the victim after the ransom in bitcoins or another cryptocurrency has been paid. Ransomware spreads like any other malware — for example, by downloading files from malicious sites or opening a file attached to a phishing email. While financial gain is the primary motive for cybercriminals, government APT groups have also used ransomware, potentially to disguise their true goals or cause disruption. Differentiating between state-sponsored and financially motivated attacks can be challenging. Overall, the increasing threat of ransomware demands closer attention. →

Criminal business model RaaS

Ransomware-as-a-service (RaaS), where developers sell access to ransomware to actors who lack the ability to create it themselves, has become increasingly common. There are various models of income distribution, including sharing a percentage of the ransom with the RaaS supplier or paying a fee for the service. Well-known RaaS vendors include LockBit and AlphV/BlackCat.

Ransomware attacks on critical infrastructure, particularly hospitals, have increased significantly globally. Attacks have targeted healthcare sectors in the US and Europe, causing operational disruptions and data loss. PikaBot malware, a modular ransomware, has been identified as a new trend, allowing for more sophisticated and versatile attacks. Double and triple extortion methods have also gained popularity, where attackers threaten to disclose sensitive information or target an organization's customers. Supply chain attacks and automated ransomware that uses artificial intelligence are on the rise. Ransomware also impacts individuals, with the StopCrypt Ransomware specifically targeting individuals with lower ransom demands.

"Attacks have targeted healthcare sectors in the US and Europe."

Threat actors use communication to put pressure on their victims

Ransomware actors communicate about their attacks through dark web or social media channels, publishing information about their victims to create public pressure for payment. These sites serve as communication and marketing channels, as well as publishing platforms for captured data. The publications often contain information about the targeted organizations, ridiculing them or highlighting their lack of security. In cases of refusal to pay, the tone of the posts can become aggressive, including identifying staff responsible for data protection failures. →

Humiliating communication is practiced especially in cases of double or triple extortion, in which case the threat actor may also contact other parties affected by the attack, such as the organization's customers or partners, and direct them to their pages. The goal is for partners to see a sample of their sensitive data and messages from criminals that the victim has not adequately protected this data and does not seem interested in recovering it.

Naturally no organization hopes to end up on these victim lists. Ending up on a victim list can attract more criminal attention and cause reputational damage. Paying the ransom may not remove the mention on the site, and correct and timely communication is important to combat public pressure. Analysis of ransomware has always been challenged by the fact that only a small percentage of all crimes end up in the public domain. Although accurate statistics are difficult to compile, authorities around the world agree that a significant number of cases remain unreported. From the point of view of criminals, acting under the radar is always desirable, which is why they try to encourage their victims to pay the ransom and keep quiet about the case.

Preventing ransomware and minimizing its effect

- Up-to-date antivirus, firewalls and a fast-patching rate of published vulnerabilities can stop the spread of malicious files.
- Staff training and good cyber hygiene practices are an effective way to prevent the threat.
- In the event of an attack, it is important to isolate the exposed network environment and take measures to investigate the incident.
- Backups play an important role in recovering from the event and the continuity of the organization's operations. However, copies of data alone are not enough, it is also critical to take into account the backup infrastructure, which can be relied on in case of problems.
- Crisis communication and communicating about the incident both internally and to stakeholders are key to minimizing reputational damage and the spread of misinformation.
- The ransom should not be paid under any circumstances. Payment does not guarantee that the data will be restored or that the data will not be leaked later. ■

ARTICLE

Exploitation of zero-day vulnerabilities on the rise

Zero-day vulnerabilities are perhaps the single most serious security threat. Simply put, a zero-day vulnerability refers to an unknown security vulnerability in an application or system. These vulnerabilities are often only revealed when the malicious actor who discovered them exploits them.

The exploitation of zero-day vulnerabilities has been on the rise for several years. Google's threat intelligence group TAG (Threat Analysis Group) and security company Mandiant published a joint report on zero-day vulnerabilities discovered last year at the turn of March and April. A total of 97 zero-day attacks were detected in 2023, more than in 2022 (62) but fewer than in the peak year of 2021 (106). Also interesting is the profile of actors exploiting zero-day vulnerabilities. According to the report, 41.4% of the actors exploiting them in 2023 were commercial spyware, 41.4% were identified state actors and the remaining 17% were financially motivated criminals. Commercial spyware refers to spyware developed by private companies, such as the high-profile Pegasus and Predator malware. Of the state actors, China is the most active actor identified. →

The recent trend in zero-day vulnerabilities has seen an increase in attacks on software providers and their products used in the business world. Cybercriminals have realized the value of exploiting vulnerabilities in these applications, especially in security applications that are often trusted. While major application developers like Google, Apple, and Microsoft still attract attention from criminals, smaller application developers have become the focus due to the ease of finding vulnerabilities in their products. Criminals have found that they can target multiple organizations with a single attack on these smaller developers. An example of this was the attack of the Russian ClOp ransomware group targeting the MOVEit data transfer application of the US company Progress Software, which affected thousands of organizations and tens of millions of individuals.

"The recent trend in zero-day vulnerabilities has seen an increase in attacks on software providers."

Another notable example from last year is the attack on another US app provider, Barracuda Networks. In this attack linked to Chinese state actors, a zero-day vulnerability discovered in Barracuda's Email Security Gateway (ESG) product, which increases the security of email transmission, the threat actor was able to infect dozens of companies and government entities across multiple continents with email-intercepting malware. It is noteworthy not only that the Chinese managed to keep their activities secret for several months, but also that the attack was so serious and advanced that Barracuda saw fit to physically replace some of the exposed network equipment with new ones. According to the company, it was otherwise impossible to guarantee that the threat actor would be deported without leaving him with a back door to the systems. →

Zero-day attacks therefore present challenges in terms of prevention, detection and recovery. However, it is not impossible to prepare for the threat. Organizations need to understand that application providers who produce solutions for many companies are becoming increasingly appealing as targets for threat actors. Even if these suppliers do everything they can, there is always a chance that a motivated and resourced threat actor will find a zero-day vulnerability. Preparedness emphasizes that organizations need to consider what data will be processed with which application and what is the backup solution if a certain product stops working. For example, in the case of the previously mentioned MOVEit attack, many victims were able to immediately establish that they were not dealing with a serious threat when they knew exactly what data had been processed with the application in question and that nothing critical had ended up in the hands of the threat actor. The worse situation was for those who had used this application produced by a third party to transfer sensitive data, and worst, for those who did not even know what data it had processed. ■

Key takeaways

1. The U.S. government has issued a warning to governmental organizations about potential Russian cyber intruders who have targeted systems by exploiting stolen data from Microsoft.

2. Public Wi-Fi networks pose security risks, including interception of sensitive data and the creation of fake networks.

3. Only about 22% of UK companies have a cyber incident plan, with small businesses being the least prepared.

4. Ransomware-as-a-service (RaaS) has become increasingly common, allowing actors without technical skills to launch attacks.

5. Zero-day vulnerabilities are dangerous security threats that refer to unknown vulnerabilities in applications or systems.

communications.sectra.com
communications@sectra.com

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

SECTRA