Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 1st Quarter 2021

Serious Vulnerabilities in MS Exchange Software

SITUATION

On March 2, Microsoft announced that it had identified and fixed four zero-day vulnerabilities in its Exchange Server software that allowed attackers to gain access to e-mails, passwords, and administrator privileges on servers.

The risk level of one of these vulnerabilities (CVE-2021-26855) was rated 9.1 on a scale of one to ten – it does not get much worse than that. Until the disclosure, few knew about these vulnerabilities, but soon after, all interested parties knew what to look for and how to exploit the vulnerabilities.

A large number of cyber groups and individual attackers began using automated tools to identify the vulnerable Exchange servers. Once they found them, the servers were compromised and infected with malware.

On March 3, Microsoft announced that the number of victims was 'limited'. On March 5, however, there were at least 30,000 victims in the United States and by March 8, more than 60,000 worldwide. This shows that the criminals acted quickly and attacked whoever they could.

ASSESSMENT

In recent months a number of high-impact cases have emerged in which components of widely used software have been compromised. In the case of Microsoft Exchange, the software manufacturer also released a critical security update to patch the vulnerabilities. Unfortunately, not all users have installed it, including many users in Estonia.

On 3 March, CERT-EE detected 80 e-mail servers in Estonia affected by the vulnerability. The owners and service providers were notified, and information security officers in the public sector and vital and important service providers were informed as well. After one week, however, two-thirds of these servers were still using unpatched software and were therefore vulnerable to attacks.

Companies and institutions whose regulations allow it should consider using some cloud-based e-mail service (Exchange Online was not affected). In this case, the service provider has the responsibility to update and patch the software.

In any case, the above is a reminder that critical security updates and relevant notifications by CERT-EE must be taken seriously. Disclosure of vulnerabilities is a starting point for both attackers and defenders, if the updates are ignored or done too late, the device can already be compromised.

Look At Your Services Through the Eyes Of An Attacker

SITUATION

In our last review, we wrote about attacks against three Estonian ministries that occurred in November. In the first months of 2021, we have seen similar attempts to compromise systems, and on a couple of occasions they have been successful. The pattern is the same: the attacker scans a web server with publicly available tools, finds security vulnerabilities, uploads malicious code, and thus gains unauthorised access to the servers. In February, we learned about two companies being compromised in that way, one which provides cloud services and software to many public sector bodies (ministries and local governments), and the other providing remote access services to public sector bodies.

The affected companies handled the incidents well: they fixed their services, informed customers, and were fully cooperating with CERT-EE. As the attack vector was familiar, CERT-EE decided to use the same tool and offer public authorities the opportunity to check their websites. The goal was to look at these websites through the eyes of an attacker and find vulnerabilities that the attacker could be tempted to exploit.

At the end of November, CERT-EE informed the information security officers on how to protect themselves from such attacks, and in March we sent a reminder to the managerial level of public authorities as well.

ASSESSMENT

The attack vector and the tactics of the attacker can be broadly compared to how common thieves operate: the attacker walks around the web, looks for unlocked or poorly secured doors, and walks in to see if there are any valuable items. Some servers do not have anything of value; some provide access to other services and important data. How to make money on the access and data – the attacker will figure that out later.

As the affected companies offer services to several public sector institutions, it may seem that the attacker is still trying to break into the servers of Estonian state institutions. However, at this point this conclusion may be premature.

Servers visible on the public Internet are scanned with various tools every second of every hour of every day. Some tools provide more efficient scanning than others. These are also more expensive and it is not profitable for attackers to test them on small institutions.

In any case, we recommend that all service owners periodically look at their servers through the eyes of an attacker using scanners or ordering penetration tests. Such services are offered by many private companies and provide a real picture of what a potential attacker sees. If an attacker scans a hundred web pages and only your one flashes red, you could well be the next target.

Supply Chain Attacks as Lessons of Basic Cyber Hygiene?

SITUATION

Over the past six months, a number of attacks have come to light where networks of various organisations were compromised through companies providing IT services. In the SolarWinds Sunburst supply chain attack, criminals had compromised the Office365 account of an employee, through which they first gained access and were able to install malware to gain access to the systems of other companies using the SolarWinds service. The Accellion attack, unveiled in February, exploited a security vulnerability in the cloud file sharing protocol through which the attackers reached hundreds of other victims around the world. Another attack disclosed in February was against Stormshield, a company providing cyber security services to the French government sector – the company was attacked through web hosting providers using an outdated version of Centreon's IT monitoring software that has not been supported for five years.

ASSESSMENT

Such supply chain attacks are not new. The NotPetya attack in 2017, considered one of the most devastating malware campaigns in the world so far, also started from a compromised update of an accounting software. When using third-party software, supply chain risks must always be considered. So far, however, there are no good mechanisms in place to verify the partner company's overall attitude towards cyber security: whether it uses multi-factor authentication throughout, what are the policies regarding security vulnerabilities or data leak, etc. These mechanisms are lacking not only in Estonia, but all over the world.

It is however premature to assess whether a better cyber hygiene in the company could have actually prevented SolarWinds type of attack by a nation state from happening.

In recent months, increased attention has been paid to supply chain security also from a legislative point of view – the new proposal for the EU's Directive on security of network and information systems (known as the NIS 2.0 Directive) requires critical infrastructure companies to adopt rules to ensure supply chain security. The importance of the supply chain is also underlined by the new cyber security strategy of the EU. In addition, new EU horizontal legislation is expected this year, which will also place more responsibility on equipment and service manufacturers.

The direct impact of the above-mentioned attacks on Estonia is limited, as the software is not generally used here. However, it is most likely only a matter of time before some large-scale supply chain attack will significantly affect Estonia and we must not only be able to assess the damage, but to identify the attack in the first place. We encourage organisations to have network monitoring and log management policies in place so that intrusions and other malicious activity could be detected. It is also worth making sure that the security audits of the contract partners have been performed and cover all areas relevant to the organisation.

DDoS Extortions Continue

SITUATION

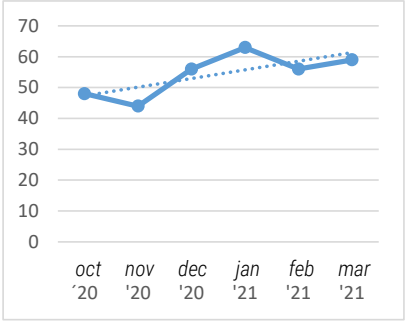
In the previous review, we wrote about Distributed Denial of Service (DDoS) attacks that took place in the autumn and aimed to extort money from selected companies. The targets included several banks and technology companies that came under attack and received an extortion letter, demanding a ransom for ending the attack. The attackers also threatened to return with new and more devastating attacks should the ransom not be paid by a certain deadline.

In early 2021, many of the same companies were attacked again. The new extortion letter also referred to previous attacks, stating that 'your payment has not reached us' and 'we are back now'. Once again, the criminals threatened to return in the future if the cryptocurrency (1–10 bitcoins depending on the company) was not paid. This wave of new incidents took place from mid-January to early February.

ASSESSMENT

Criminals have used denial-of-service attacks for extortion before, but it is not common to return to the same companies in a relatively short time. The attacks in the autumn and at the beginning of the year seem to be carried out by the same criminal group (they use the same cryptocurrency wallet address and there were also other indications that this was a deliberate repeat activity). According to CERT-EE, similar extortion letters and repeat attacks have been seen in at least five other European countries. Both the scale of the attacks and the variety of methods used point to a relatively good infrastructure of the criminals. As the bitcoin value has also multiplied since the autumn, they are probably highly motivated to try again.

Altogether, such extortions are not very common in Estonia – about ten companies have been affected so far and the public sector has not been affected at all. At the same time, it is likely that companies that have already received an extortion letter will sooner or later be targeted again, and the grouping seems to have the resources to carry out its threats. To the best of our knowledge, no Estonian company has paid the ransom, and after the initial attacks many have improved their readiness to cope with DDoS attacks. This is very sensible, as DDoS attacks of various intensity take place in Estonian cyberspace every month and their number is on a slight growth trend.



Number of DDoS attacks against unique IP addresses in Estonia

GOING WELL:

In February, attentive employees of an Estonian construction company prevented a Business Email Compromise scam which could have cost the company more than 900,000 euros. One of the company's e-mail accounts had been hacked and criminals began monitoring communications with suppliers. By hijacking the conversation at the right time and changing the account details of the bills, the criminals hoped to transfer the money to a bank account outside the European Union instead. However, this plan failed because the employees noticed the scam and did not authorise the payments.

COULD BE IMPROVED:

Remote Desktop Protocol software, known as RDP, is widely used in Estonia to connect to work network from home, but is not always appropriately secured. If RDP ports are left exposed to the internet, your computer or server is accessible from all over the world. Every month CERT-EE receives information of several incidents where the attacker has used the RDP to breach a system; in March, a government agency was also affected by such an attack.

This summary was prepared by the Cyber Security Branch of the Estonian Information System Authority (RIA) with the aim of explaining the trends of cyber threats to the widest possible audience, including readers outside Estonia. The situation in cyberspace is analysed in more detail in monthly summaries. CERT-EE distributes more technical recommendations at trainings and on RIA's website.