Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 4th Quarter 2020

Three Ministries Breached Demonstrating Need For More Robust Cyber Security Measures

SITUATION

In November, the Information System Authority (RIA) identified three similar attacks on Estonian state IT infrastructure. The attacks targeted the servers of the Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, and the Ministry of Foreign Affairs. All three attacks shared the same pattern: the servers hosting the websites were attacked in an attempt to exploit vulnerabilities in their configuration.

In the case of the Ministry of Economic Affairs and Communications, attackers managed to gain access to several servers within its jurisdiction and several hundred gigabytes of data were stolen. The Ministry of Social Affairs attack saw the cyber criminals accessing COVID-19 related data on 9,158 individuals, via the Health and Welfare Information Systems Center (TEHIK). TEHIK was able to block the attacker within hours and the Health Board informed the people concerned. The Ministry of Foreign Affairs got off the easiest, as the criminals did not get past their website and were unable to access any sensitive information.

Despite the scale of the incident, Estonian e-services were not jeopardized and our digital state functioned as usual. We informed other state agencies, local governments, and providers of vital services about the identified vulnerabilities of web servers and issued guidance on how to eliminate them.

ASSESSMENT

Technologies evolve very fast, allowing for more possibilities to abuse them. New vulnerabilities are discovered almost every week and the November attacks reminded once again that criminals are actually exploiting them. A successful cyber attack can result in data loss and/or a leak of sensitive information; access to the system also enables gathering information that will eventually help to move on from the web server and compromise other parts of the information system. In addition to information, an attacker may also be interested in money, planning further ransom attacks, or attempting to sell the data. Several public authorities made joint efforts to minimise the impact of the attacks and to prevent new ones from happening. Nonetheless, the full impact of data theft may materialise months or even years later.

What lessons can we learn from this? The attacks show that even government agencies, which are subject to strict information security rules, can be seriously hit by cyber attacks.

We see the same from international news – in December, the public learned about a cyber attack through SolarWinds Orion software updates, which compromised the information systems of thousands of organisations around the world, including those of several US government agencies. Although complete security against cyber attacks cannot be achieved, investment in cyber security must be consistent and systematic and a workable crisis management plan must be in place to respond to a critical incident.

We also advise to create a complete overview of your information systems – list the equipment and software that is being used, list all user accounts and what rights they have, and have a log management system in place to quickly detect anomalies. Although the above sounds elementary, the situation is often far from perfect, including old legacy systems and temporary quick solutions where cyber security falls behind other priorities. Cyber security in today's digital age is expensive, annoying, and largely invisible, but it is becoming indispensable, as at the end of the day it is cheaper for both companies and public authorities to prevent problems than to deal with the damage afterwards.

Distributed Denial-of-Service Attacks for Extortion Purposes

SITUATION

In the last quarter, we received several reports of attempts to extort money from companies with distributed denial-of-service (DDoS) attacks. Companies received letters in which criminals threatened to carry out a DDoS attack if the company did not pay a required ransom. In most cases, this was accompanied by a test attack and a threat of a more serious attack if the ransom is not paid on time. To increase their credibility, the criminals claimed to be affiliated with Fancy Bear or some other notorious cyber group and referred to previous attacks carried out by these groups that had caused significant economic loss. Ransom was demanded in cryptocurrencies and ranged from 10,000 to 400,000 euros. The attacks were mostly aimed at either telecommunications companies or banks, the latter being asked for the largest ransom payments. To the best of our knowledge, no companies agreed to the demands of the attackers, nor do we have any reports of repeat attacks at the time and in volume promised by the criminals.

ASSESSMENT

These attacks were part of a global string of extortion which began to spread in August and reached Estonia in autumn. The aim of the criminals is to make a quick profit, and there is no real connection with the well-known groups, such as Fancy Bear, Cozy Bear, or the Armada Collective. The attacks are targeted and the targets mostly operate in the financial, telecommunications, and e-commerce sectors, i.e. sectors where the commercial impact of the threat of a large-scale attack would be greater.

The impact of the attacks seen in Estonia varied depending on the size of the attack and the existence and effectiveness of countermeasures. In some cases, the attack resulted in disruptions which affected the website of the company and lasted only a few minutes; however, the attack which had the biggest impact (the parent company of a bank operating in Estonia was attacked) rendered the payment terminals of the bank inoperable for a few hours during peak time, which prevented or postponed transactions worth millions of euros.

With regards to DDoS attacks in general, we received notifications about a total of approximately 140 attacks against Estonian IP addresses in the last quarter of 2020, which is somewhat more than in the third quarter. DDoS as a Service tools have grown in popularity due to their availability and relatively low cost for criminals. Therefore, we anticipate that the number of DDoS attacks will continue to increase this year, and we recommend to make the necessary investments in relevant countermeasures.

Most Ransomware Incidents in Estonia Related to the Remote Desktop Protocol

SITUATION

At the end of 2018, in our first quarterly review, we wrote about ransomware attacks via network connections that had been left open for the Remote Desktop Protocol (RDP). Two years later, the situation has not changed: CERT-EE receives a number of reports of ransomware incidents each month where, at first, the attacked institution is unable tell how the attackers could gain access, but after further analysis, it is concluded that access was probably obtained by exploiting the vulnerabilities of the Remote Desktop Protocol. Ransomware incidents caused by pirated software or emails which contained malware have mainly been reported by private individuals.

Three-quarters of the ransomware incidents reported to us in 2020 were definitely or most likely committed via RDP. Among the targeted victims were schools, family health centres, manufacturing companies, accommodation establishments, car dealers and, naturally, private individuals. Fortunately these attacks did not lead to major financial damage; in most cases the main loss were the man-hours spent on recovering the system.

ASSESSMENT

By paying ransom, many companies around the world have enabled criminals to improve their malware, upgrade their infrastructure, and avoid detention. Taking a closer look at the trends in ransomware attacks, it is noticeable that using malware that has been sent to victims by e-mail is becoming increasingly popular. One such malware strain is Emotet, which is widespread also in Estonia and offers services to other malware groups, including criminals running ransomware operations. Victims receive phishing e-mails which refer to malware often stored in public Google, Microsoft or Amazon clouds, making the e-mails look more legitimate. Therefore, it is crucial to continuously train staff to recognise phishing e-mails and to not click on strange links.

In addition to new types of attack methods, it is also necessary to pay attention to the threats that target Estonian companies and institutions on a daily basis. Two years ago, we found that precautionary measures were often introduced only after a ransomware incident had taken place – RDP has been known as a possible attack vector since 2016 and earlier. Due to the surge in remote work and increase in RDP usage, we continuously urge people and organisations to make sure that their RDPs are configured properly and not exposed to the Internet.

NIS 2.0: European Union Revises Directive on Security of Network and Information Systems

In mid-December, the European Commission presented its vision to the Member States for the revised Directive on Security of Network and Information Systems, commonly known as the NIS Directive. The current NIS directive entered into force in 2016, and the revised version, NIS 2.0, will probably take effect in about two to three years. The aim of the directive is to raise the overall minimum level of cyber security in the EU Member States and to take into account the growing interdependence of different services and sectors. The pandemic has also highlighted the need to better protect medical research and development and other fields related to it. As the level of cyber security varies greatly from country to country, as does the vision for achieving greater strategic autonomy, intense negotiations lie ahead.

The main changes concern the scope of the directive, the exchange of information, security requirements, and fines. While the current NIS Directive gives Member States quite a lot of flexibility to define which companies need to comply with the requirements of the Directive, NIS 2.0 introduces a size criterion: the requirements of the directive must apply to medium-sized (50+ employees) and large companies. There are also exceptions – companies which should be subject to the requirements regardless of their size, e.g. if they are the only provider in their sector or if they provide an important service at a regional or national level. At first glance, it seems that the current flexible but straightforward system will become more rigid and general.

According to the proposal, institutions would be classified based on the level of importance of their service, as well as the level of interdependency – if the work of one physical infrastructure entity depends on a digital infrastructure company, then both can be considered equally important. In addition to essential entities, the concept of an important entity has been created. The difference between essential and important entities lies in supervision, where important entities – unlike essential entities – cannot be subject to *ex ante* supervision. Essential entities would include for example entities manufacturing pharmaceutical products and medical devices, public administration entities, and entities providing space-based services; important entities would include most of the industrial sector, food production and manufacture of machinery and electronics, processing industry, as well as social media platforms. Compared to the current NIS Directive, the scope would therefore be significantly wider.

Meeting the updated security requirements requires that the management bodies of essential entities are aware of cyber security measures and risks and receive basic cyber security training. There may also be additional obligations for certain entities to use only certified products. The directive would also introduce drastic changes in the punitive measure which would be harmonised with the General Data Protection Regulation and provide for fines of up to 10,000,000 euros or up to 2% of the total annual turnover for non-compliance with the requirements.

Finding a fair balance between efficient measures to improve cyber security across the EU and avoiding over-regulation and excessive administrative burden will be a challenge for the forthcoming negotiations. RIA will analyse the effects of the Commission's proposal and submit the initial assessment to the Government in February.

GOING WELL: ↗

Phishing attempts sharing a common pattern, in which criminals tried to lure victims into providing their Smart-ID or Mobile-ID codes needed to access the Internet bank, have been a matter of concern for us since 2019. Phishing emails and messages reached up to 100,000 people in Estonia and the criminals managed to gain access to at least 400 accounts. On September 28, three men suspected of conducting phishing campaigns were arrested in Romania as part of international police cooperation. We did not expect this to completely eliminate the phishing attempts for bank details, but we are glad to see that the number of such scams has fallen significantly in Q4 of 2020.

COULD BE IMPROVED: ⚠

On October 20, members of the US Democratic Party received a threatening email: 'Vote for Trump or else!' The emails, which tried to influence the elections, were apparently sent from info@officialproudboys.com, but the metadata revealed that a server located in Estonia was used for sending the emails. The attackers exploited the vulnerability of a website belonging to an Estonian publishing company and infected it with a malicious code which was used for sending the emails. This embarrassing incident could have happened anywhere, but happened in Estonia and highlighted the need to properly maintain websites and servers – keep the software updated and security holes patched.

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 www.ria.ee.