Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 2nd Quarter 2020

New Trends in Ransomware: Data Theft

SITUATION

Although ransomware attacks are no longer talked about as much as in 2017–2018, they have not disappeared. Incidents in recent months confirm that the attackers have made their tactics more brutal: in addition to encrypting data, it is also stolen and threatened to be disclosed.

A classic ransomware attack usually had three steps:

1. The attacker installs ransomware on the victim's computer or server. They increasingly use vulnerable remote desktop protocols or weak or known passwords for access. Malware is also distributed in e-mails.

2. The ransomware encrypts some of the files on the computers or servers. After that, the victim can no longer open the files.

3. The attacker demands a ransom for data recovery, i.e. for a decryption key, usually in some cryptocurrency (such as Bitcoin).

As organisations have become more aware of the importance of backup and better protect their data, they do not pay the ransom because encrypted data can be recovered without a decryption key. As a result, the perpetrators have added a fourth step: during the process the data is stolen and the victim is threatened with disclosure if they do not pay.

CERT-EE is aware that such a ransomware attack recently struck an international medical institution (not located in Estonia). When the victim refused to pay for the decryption key, the attackers announced that they would disclose the data stolen during the attack and carried out the threat. As a result, sensitive personal data of patients was leaked, such as names, dates of birth, notes on allergies, test results, etc.

Data theft complicates and slows down ransomware attacks and increases the likelihood of early detection, but the ability to obtain ransom money also from organisations that have robust recovery plans has increased the proportion of such attacks. According to the French cybersecurity agency ANSSI, attacks involving data theft and the threat of their disclosure account for almost a quarter of the ransomware attacks known to them.

ASSESSMENT

All organisations should assume that, in the event of a ransomware attack, the data on their devices is not only encrypted but also stolen and may be disclosed. Therefore, backing up data is not enough to combat ransomware attacks.

The amounts demanded by the criminals amount to millions of euros. Victims often pay the ransom due to the fear of fines under the European Data Protection Regulation (GDPR), should personal data held by the organisation leak. Criminals are also increasingly referring to fines for GDPR violations to persuade their victims to pay. Backups should certainly continue to be made, but it is no longer possible to defend oneself against ransomware attacks in this way.

Working From Home: New Accounts, Old Passwords

SITUATION

Due to the emergency situation and lockdowns to prevent the spread of the COVID-19 pandemic, people were left to work and study at home, which meant that they urgently needed to create new accounts on several platforms. In rare cases, they only had to use only a few new services, but in the case of parents of children attending several school levels, we have also heard of dozens of new accounts needed for work and study.

Experience has shown that not enough time is devoted to creating the passwords of new accounts, and passwords already in use elsewhere are reused (as confirmed by Google's 2019 US study, which shows that 65% of people use the same password in several or all of their accounts). However, this means that if a password is leaked through one environment, all other accounts with the same password are automatically compromised.

Large-scale data leaks continue everywhere, from airlines to children's virtual playrooms. Although data theft is quite common, people's behaviour in cyberspace remains risky – one of the main risks here is the re-use of passwords on different platforms.

ASSESSMENT

Strong passwords and different passwords for different environments are an important part of cyber hygiene, and we encourage everyone to take a moment and review our personal password habits. During the emergency situation, the priority was to adapt to the situation and get used to different online environments. Now, however, people can think about your future internet habits calmly, organise their accounts, and make them more secure.

Estonian Information System Authority has provided recommendations for creating a secure user account. As many companies accelerated the process of moving their business online in the context of the emergency situation and are selling services through a website, it is also appropriate to review the reminder to the service provider.

Our experience shows that leaked passwords and stolen data are often not realised immediately, but only after several months, sometimes even later. Therefore, users may not be aware that their user data has been leaked and personal data and accounts may be at risk. In terms of cyber hygiene, it is certainly safer to use a separate password for each account and to use two-step authentication in more important environments with sensitive information. We recommend password managers, special software for managing different passwords (there are many of them, but the best known are KeePass, LastPass, or 1Password).

The Risk of Denial-Of-Service Attacks Persists

SITUATION

In April and early May, we saw more denial-of-service (DDoS) attacks against Estonian websites than usual, lasting from a few minutes to almost a day. The longer attacks took place against two financial companies, as a result of which both companies' websites were down for customers throughout the working day. Shorter attacks took aim at the websites in the transport sector, public services, and vital service providers. Although services were quickly restored in the event of the short-term attacks, a half-hour service outage in a widely used e-learning environment, for example, caused quite a lot of inconvenience to nearly ten thousand users during the emergency situation.

Various denial-of-service attacks take place constantly, but the attacks in the second quarter caught our attention for two reasons. Firstly, there were more attacks over a short period of time (approximately four weeks) than usual, and as this was also an emergency situation where people used all kinds of e-services more, some attacks also had a greater impact than usual. Secondly, the handwriting of some attacks was similar: HTTP Get queries were made, the attackers had the same or a similar user agent, and the objects of the attacks were popular and important websites in Estonia.

ASSESSMENT

In these cases, it is not possible to draw sufficient conclusions about the purpose of the attacks or the attacker, but this shows that the risk of denial-of-service attacks must continue to be taken very seriously. The attacks are usually carried out using either botnets or networks of compromised devices, and in this wave of attacks, CERT-EE found that in some cases, compromised Miktrotik routers were used around the world (including in Estonia). The compromise could probably have been avoided if the router's software had been updated in time – this is why we repeat the need to update the software of all devices connected to the Internet regularly.

All around the world the trend of denial-of-service attacks this year seems to be on the rise, both in terms of amounts and impact. In addition to previously known vulnerabilities in both software and hardware, new vulnerabilities are constantly being discovered that may facilitate such attacks. For example in May Israeli researchers discovered a vulnerability in the global Domain Name System (DNS) service that could potentially be used to carry out attacks with a very small number of devices with a very high amplification effect.

Housekeeping: Less Noise, Better Threat Picture

Our international partners may notice a downward trend in the number of incidents reported by the Estonian Information System Authority in the coming months. This will be due to a change in how we manage automated notices regarding infected systems discovered during scanning (by us or by our international partners). Most of these automated notices are not recorded in the incident statistics that we report, some still are. We will be integrating the few notices which today still need hands-on interventions onto the same automated platform.

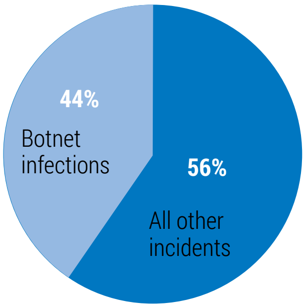
This change demonstrates the increased visibility into the Estonian cyber threat landscape. Since the summer of 2019, CERT-EE has sent such automated notifications to Estonian telecommunications companies, web service hosts, and institutions managing their own networks about various vulnerable devices/settings in the networks. At the moment, CERT-EE receives information on about 3,000 infections a day, which affects more than 700 servers and computers in the Estonian IP-range.

More Notices More Often

The more we integrate such feeds into our systems, the better can serve our constituents. But reflecting each individual notification as a cyber security incident only makes the threat picture less clear. For example, from mid-May to mid-June, within a 30 day window we have notified Estonian service providers of 103,000 infections. However, analysing the numbers, we can see that about 86,000 of them were associated with only three IP addresses, and we know of a total of 1,701 different malicious IP addresses.

The integration of some of the incidents onto the automated platform will initially show a noticeable decline in the amount of incidents (estimated at about 50%), but as a result of the change, our reports will reflect the threat landscape in Estonian cyberspace more clearly. Malware detection and mitigation has gotten better over time but some devices are infected again and again after having been cleaned. This is an ongoing process and reporting every botnet and malware infection in the Estonian IP-space will only muddy the picture. We plan to make summaries of botnets and infections in the future as well, but in a different way, showing the trends of infections over a certain period of time and focusing on their dynamics.

Incidents registered by CERT-EE in 2020



In 2020 44% of all registered incidents that affect the confidentiality, availability or integrity of systems or data are related to systems infected by certain botnets.

GOING WELL:

Although the emergency situation connected to the COVID-19 pandemic that lasted from mid-March to mid-May put a greater strain on both e-service users and service providers, it did not lead to more cyber incidents or incidents with a higher impact than usual for Estonia. We did not have targeted attacks on the medical sector which took place in some European countries, and we were left largely untouched by COVID-19 scams, which caused great financial damage.

COULD BE BETTER: ⚠

On June 30, support ended for the 1x version of the Magento software, which is a very widely used website and online store platform software in Estonia. According to CERT-EE, approximately three of four Estonian online shops use Magento software, and to continue secure trading it is necessary to switch to a new version. CERT-EE also sent a respective notification to service providers in May. However many have not done so (even in the beginning of July) including e-shops that sell food and consumer goods. This means that the customers' credit card information may be at risk. Because hackers have successfully exploited Magento's previous security vulnerabilities in other parts of the world, Visa and Mastercard have also raised the issue.

This summary was prepared by the Cyber Security Branch of the Estonian Information System Authority 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 by the Cyber Security Branch of the Information System Authority in monthly summaries. CERT-EE distributes more technical recommendations at trainings and on the website of the Information System Authority.