Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 3rd Quarter 2020

Do Not Forget Updates When Using Coronavirus Tracking App HOIA

SITUATION

Starting August 20, Estonian residents can download the mobile application HOIA, which aims to help limit the spread of the coronavirus. The application notifies the user if the user has been in close contact with an infected person. Users' phones exchange anonymous codes via Bluetooth, and the phone of a person who has marked themselves as COVID-positive warns those who have been in close contact with them. Neither the Estonian government agencies, the creators of the application, nor phone manufacturers can find out who was in close contact with whom, or who has declared themselves ill. Furthermore, the notification does not disclose when and for how long the contact with the COVID-positive person occurred, so there is no way to identify the infected person. Thus, the creators of the application have already taken into account the privacy and protection of personal data when developing the application.

The application has also successfully passed the appropriate security testing.

Other EU Member States are developing similar applications (16 applications are currently underway and four are almost completed). These applications are also based on information shared via Bluetooth and possible alerts. The next step is to create interoperability between applications in different Member States to achieve a situation where, for example, HOIA also works in Germany and vice versa. Bluetooth-based COVID applications are also used in many other countries, such as Singapore, India, Israel, the United States, and Australia.

ASSESSMENT

The only significant cyber security risk related to the HOIA app is the need to keep Bluetooth data turned on at all times. Potential Bluetooth security vulnerabilities have been an issue for many years and much has been written about them.

These risks can be mitigated to a reasonable level for the average user. The most important thing is to keep both your phone's operating system and the applications up to date. From a safety perspective in general, and not just in the context of HOIA, it is not safe to use devices that are no longer supported by the manufacturer and therefore do not receive security updates. This includes models older than Apple's iPhone 6S or iPhone SE (2016). For Android devices, the situation is more complex, as some of them only receive updates for 2–3 years after launch. In updated phones, the chances of exploiting Bluetooth are minimal, as manufacturers regularly patch vulnerabilities.

Given the spread of the coronavirus and the increase in the number of infections in the fall, as well as the approaching flu season, RIA recommends everyone to contribute to the fight against the virus by downloading and using the HOIA application. Our general recommendation is to not use devices that do not receive software updates. However, if you are using an older device, you should be more cautious about both data communication and Bluetooth. Overall, we currently assess the societal benefits of using the HOIA application to outweigh the mostly theoretical risks of using Bluetooth (CERT-EE has not registered any incidents regarding the use or abuse of Bluetooth technology).

Cyber Fraud and Ransomware Attacks Continue

SITUATION

In the 3rd quarter, we continued to receive numerous reports of business e-mail compromise (BEC), salary account fraud, and ransomware attacks every week. The losses range from a few thousand to tens of thousands of euros. The largest one-off loss was 41,000 euros lost by the business partner of a South Estonian company through BEC – where criminals intercepted and changed the bank account details on invoices.

Although scammers target both large and small companies, the general rule is that the smaller the company, the less attention is paid to cyber security and the easier it is to attack them. Most criminals are rational: their goal is to make as much profit as possible by spending as little time and money as possible.

Many of the victims of cyber fraud in Estonia are small and medium-sized enterprises that do not have a separate information security officer or IT team. However, they too can protect themselves better and it all starts with raising awareness of such scams. In September, we launched an awareness raising campaign to draw attention to the most common scams and advise SME-s on how to prevent them.

ASSESSMENT

We do not have the naive assumption that Estonian companies will be safe by the end of October thanks to the awareness raising campaign. The more digital the communication within and between companies, the higher the likelihood of online fraud.

Frauds have become simpler as well. Hacking into a company's IT systems can be a relatively complex, costly, and time-consuming endeavour, plus it entails the risk of discovery. It is much easier to send an e-mail to the company's accountant or human resources manager with a request to change the bank account number used to pay the salary. Changing the name of the sender of an e-mail can be done in a matter of seconds. Changing the sender's actual e-mail address is a little trickier, but is often not necessary. In most cases, the recipient of the e-mail does not bother to check the sender's address if their name is familiar. A similar logic applies to invoice fraud: we have seen schemes that do not even attempt compromising e-mail conversations or their targets. Instead, the criminals send an e-mail based on publicly available data to some companies with a proposal to change a bank account number of a sub-contractor.

With regard to ransomware, we need to brace for even greater damages. As a result of recent successful attacks many victims around the world have decided to pay the criminals, as a result of which ransomware groups have been able to significantly develop their tactics, techniques and procedures. Currently, the most effective protection against ransomware attacks is having a backup (in an offline site) of all important data and a robust plan for recovery. More attention should be paid to prevent attacks – to watch out for phishing pages and the Emotet-style malware, use multi-factor authentication, and keep your systems up to date.

Emotet's Latest Wave Has Reached Estonia, Impact To Be Seen Later

SITUATION

The Emotet malware which resurfaced in July also reached the Estonian cyberspace to a greater extent in August. We have received reports of more than a hundred infections in various sectors: trade, transport, construction, as well as one smaller government agency. Emotet is mainly spread through e-mail campaigns via macro-enabled attachments (sometimes links), using contacts as well as e-mail threads found on already infected accounts. We have seen different variants:

An e-mail with an attachment and a concise message in English is sent as a follow-up to a correspondence from a familiar person or trusted institution. The message may be, for example, 'Please confirm' or 'I would like to seek your advice on this'. In some cases, the e-mail consists of a previous conversation that was simply resent with the attachment. The attachment looks like a regular Word file that, when opened, shows that certain macro content is disabled. To enable it, it prompts you to click on 'Enable Content'.

In another variant, an additional click was required to open the attachment on the pretext that the document had been created on an iOS operating system, which the user's computer did not support. In a third variant, the user had to click 'Enable editing' and then 'Enable content', as the document was said to have been created using a Windows 10 mobile application. In any case, opening the attachment and making the required clicks will infect your computer with malware. Typically to Emotet, there are initially no visible signs of infection for the user.

Emotet is a Trojan that infects your device and creates remote access to it by third parties. Access allows the criminals to steal your data, such as the contents of your mailbox, and use it to spread the malware. Infected devices also form botnets that are resold as a service to other malicious groups to carry out cyber-attacks of varying scales and purposes.

ASSESSMENT

Emotet's initial goal seems to be spreading as widely as possible. This is facilitated by the fact that the sender of the e-mail, the subject line and the extension of the attached file all seem credible at first glance. Furthermore, as the malware often spreads itself by re-sending actual conversations, the content of the e-mail may be in Estonian and familiar too. More advanced antivirus programs can often detect attachments containing Emotet so that they do not reach the end user, but the malware can quickly change its characteristics too. Therefore, general awareness and caution are needed to prevent the wider spread.

The risks of infection with this malware are quite varied. In the past, Emotet has been used to install malware such as Trickbot and Qbot, which steal the users' bank data. In other cases the malware has been used to carry out ransomware attacks. However, there can be another costly consequence: data leak. As Emotet uses stolen e-mails and data to spread, the personal data held by a company may be leaked. The companies in Estonia have an obligation to notify the Data Protection Inspectorate of all incidents related to personal data leaks.

Sending out malicious e-mails does not reveal all infected devices – in fact, the data leak or ransomware attack may only materialise after a while, when the criminals have a good overview of which organisations they have been able to infect. It will be quite difficult to estimate how many future incidents can be linked back to the current wave of Emotet.

GOING WELL:

In June, we published a threat assessment of the BGP (Border Gateway Protocol) hijacking risks and recommended that companies use the RPKI (Resource Public Key Infrastructure) validation solution to mitigate them. By now, the use of RPKI has grown significantly: while at the end of June, only 25% of all Estonian IP addresses were protected by RPKI, it has risen to almost 75% today. This makes the Estonian cyberspace less vulnerable to BGP hijacking.

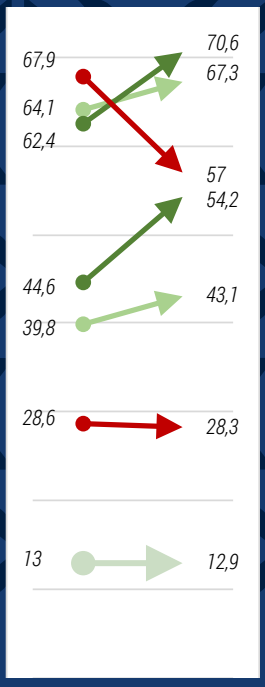
COULD BE IMPROVED:

In the first quarter of the year, we discovered that many of the notifications that CERT-EE sends to telecommunications companies, web service providers, and their network operators about vulnerabilities or network abuses often do not reach the end user. Unfortunately, the situation has not improved significantly. Every week we receive reports of incidents that could have been prevented if our notifications had been duly taken into account. We recommend that people pay more attention to CERT-EE notifications, so they will save time and stress less later.

Estonians' Cyber Hygiene Improves Slowly

For the second year in a row, Statistics Estonia asked Estonians about their cyber hygiene habits.

Q: What have you done for personal security or privacy on the Internet or in an application?



1.	Checked links and attachments in unexpected e-mails or e-mails from unknown senders before opening them	70,6% (+8,2)
2.	Strengthened passwords or using different passwords (including passwords that surpass minimum requirements, regularly changing, etc.)	67,3% (+3,2)
3.	Used security programs or applications (e.g. anti-virus, anti-spyware, firewall)	57% (-10,9)
4.	Avoided using the Internet on somebody else's computer or device	54,2% (+9,6)
5.	Researched the background of the company/service provider before using their new device/application/service or ordering goods from them (e.g. e-shop, taxi applications)	43,1% (+3,3)
6.	Changed the security settings of the Internet browser/social network/ application	28,3% (-0,3)
	I have not done any of these	12,9% (-0,1)

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.