



# Trends and Challenges in Cyber Security

Quarterly Assessment, 4th Quarter 2018

## Corporate Fraud Attempts Using Information From Compromised Accounts

### SITUATION:

We have observed a wave of fraudulent e-mails where attackers are using compromised e-mail accounts and e-mail threads to attempt fraud. An example of this was a large Estonian enterprise who first notified us of a breach of their employee's e-mail account. Initially the compromised account was used to distribute hundreds of phishing e-mails, but at the same time the contents of the account were copied and used for a new attack months later. This looked like a normal reply to an e-mail thread where the Estonian company asked a partner to send their bank transfers to a new account.

We have seen similar attacks in Estonia the other way around as well. At one point of the e-mail thread a contractor located in Asia asks an Estonian company to redirect transfers to another bank account. Only later it is discovered that a third party is exchanging e-mails with both sides trying to defraud both of them. This means that at a certain point neither partner is aware that their e-mail exchange has been hijacked.

### ANALYSIS:

These types of attacks are much more complex than the familiar CEO fraud operation (a simple sentence translated into Estonian asking "Can we send 29k now?") which still finds victims in Estonia. The goal seems to be finding a larger payoff compared to targeting private individuals. To achieve this goal, criminals are ready to devote more resources into the scheme, giving themselves time to monitor the e-mail thread to spot the right time to intervene.

This type of attack is difficult to uncover and protect against, since the fraudulent messages are coming from a trusted partner and are embedded within a trusted e-mail thread. There have been instances where the fraudsters have hijacked the conversation to other e-mail addresses to keep the employees (who still have access to the e-mail accounts) in the dark – this may increase the probability of tipping the victims off. Nevertheless the sophistication of this attack should alarm any entrepreneur whose partner is asking them to change payment details in the middle of a transaction or at the last minute.

## Fewer Individuals, More Companies: Office 365 Users Targeted

### SITUATION:

Estonian companies using Microsoft Office 365 products have notified us of attempts and breaches of their e-mail accounts. Criminals have used Office 365 e-mail applications to track companies' e-mail threads for longer periods of time to use intercepted e-mails in their fraud attempts as discussed earlier.

Our counterpart in neighboring Finland, the Finnish National Cyber Security Center released security alerts about the same issues of Office 365 breaches during the summer, updating it in October. At the same time, multiple cyber security companies have issued warnings about phishing attempts and account compromises regarding Office 365.

### ANALYSIS

Microsoft products, including the cloud-based Office 365 are popular among Estonian companies because of their reputation, and the pricing of an enterprise-focused e-mail solution. This e-mail platform will remain an attractive attack vector for criminals because it remains attractive to companies. The product provides company-wide account directories that could provide attackers with additional potential victims who have access to fiscal decisions, forwarding rules to hide their long-term surveillance and (when so configured) an ability to bypass multi-factor authentication.

Microsoft has beefed up the security on their Office 365 platform over the years. For example they reported important improvements on blocking phishing e-mails. But the attacks show that the criminals are not that much interested in the platform but its users – the corporate accounts. Private individuals and their individual security behavior is still the first access point for attackers looking for a bigger payoff.

## What To Do If Your Corporate Accounts Are Compromised?

All instances of compromised corporate e-mail accounts should be considered very carefully by the affected parties because this may lead to attempts to defraud your partners.

### NOTIFY YOUR PARTNERS

We have observed that criminals may wait for months before they will intercept and interfere in business e-mail threads using your name. If an account has been compromised, it would be responsible to notify your partners about possible risk that your business name could be used to attempt fraud – for example if someone is asking to change banking details on your behalf. This type of a major revision of transaction details should be confirmed through other channels. Notifying your partners lets them know you take security seriously.

### TAKE CARE OF YOUR (DOMAIN) NAME

SPF, DKIM and DMARC may sound like obscure acronyms but for security experts they are simple and low-cost tools that can lower the risk of bad actors using your domain name to distribute malware or phishing e-mails. Make life much more difficult for them and ask your IT partner to consider these technologies.

### FIND WAYS TO IMPLEMENT MULTI-FACTOR AUTHENTICATION

More and more service providers have made multi-factor authentication available to customers. Think of ways that your company could implement multi-factor authentication when logging into e-mail solutions or internal networks so that even if passwords are breached, the attackers would not be able to access your systems easily.

# 64%

Incidents\* registered by CERT-EE this year are reports of malware.

## (A Bit) More Sophisticated Ransomware Attacks

### SITUATION:

The successful ransomware attacks that we have observed over the summer and into the fall have often been carried out using connections left open for Remote Desktop Protocol – ports often used by administrators to access internal networks remotely. It is possible to scan for these open services automatically.

After finding the open ports threat actors will attempt to brute force guess credentials to the system. At times these attacks succeed because of the human factor involved – sometimes the passwords are just not complex enough. After gaining access to the internal network, criminals will manually upload the ransomware and run it.

### ANALYSIS:

There are different ways to lower the risk of a successful ransomware incident but despite its wide impact, companies and institutions often start implementing precautions only after the successful attack. We have been aware of the Remote Desktop Protocol ports as a threat vector in ransomware attacks since 2016, this knowledge has been widely shared within the community but we keep getting reports about these attacks more than two years later. The FBI deemed it necessary to issue another guidance regarding RDP vulnerability as late as September 2018 to advise users to disable the service if it is not needed.

We intend to keep informing Estonian companies, institutions and users of these types of vulnerabilities as long as we consider them a threat to information systems in Estonia, though we understand this may not solve the problem in the near future. We expect that criminals will keep looking for small and medium sized companies or institutions that do not have the resources to protect their connections in the way that larger companies do.

This also affirms the previously discussed trend of criminals turning their attention toward companies with more financial resources rather than private individuals.

*\*For CERT-EE, an incident is a situation where the confidentiality, integrity or the availability of the information system and/or the information of an organisation, institution or a person is violated.*

# 13%

Increase in incidents\* registered by CERT-EE in 9 months of 2018 compared to 2017.

## Exploiting Known Vulnerabilities Through “Forgotten” Devices

### SITUATION:

All through the year 2018 we have seen advisories regarding vulnerabilities in home and small-office routers made by Linksys, Mikrotik, Netgear and others. These software vulnerabilities allow threat actors to mine cryptocurrencies, to collect data that flows through the devices or to mask an origin point of an attack.

In July of 2018 CERT-EE also advised users of Mikrotik routers to update their software. Despite the advisory, we receive reports of unpatched routers still online on public and private networks.

### ANALYSIS:

Despite the fact that the software of these devices can be patched with an update, threat actors are counting on the fact that users and administrators of these devices either may not notice the update, do not see the update as essential or do not even know that a vulnerable device is online within their administered networks.

The releases to patches to discovered vulnerabilities are closely followed not just by cyber security experts but also by bad actors intending to exploit those vulnerabilities. As soon as the details of a vulnerability are released, there will be an attempt to reverse-engineer an exploit for it. Speed is of the essence here because if threat actors are able to deploy an exploit quickly, it may reach many information systems that have not been patched yet.

As the amount of connected devices grows in the growing era of the Internet of Things (IoT), we can expect a growing trend of exploiting known vulnerabilities through forgotten or just unpatched systems. If the devices do not patch automatically and if they are being used more by novice (or regular) users not expert-level users, we expect an even smaller share of vulnerable devices to be patched within a reasonable timeframe or at all.

### IMPROVEMENT OBSERVED:

## Primary Care Doctors and Healthcare Centers Getting More Attention

Compared to large hospitals and national health information systems, the smaller privately owned practices of primary care doctors (also known in Estonia as family doctors) have been struggling with the cyber security of their businesses. This is why RIA is focusing more on helping them.

- We have completed a review of the cyber security of the information systems that family doctors are using all across Estonia.
- Family doctors and other healthcare workers at their practices now have access to a cyber hygiene digital testing platform which had been available only to the government sector.
- Family doctor centers and associations also invited volunteer experts to give lectures on cyber security within the Cyber Security Month campaign in October.

### LACKS IMPROVEMENT:

## Estonian Companies and Institutions Still Vulnerable to E-mail Spoofing

Cyber incidents often start from e-mails that look like they come from a trusted source. There are free and effective solutions to lower this risk (search for SPF, DKIM, DMARC and ask your e-mail or domain service provider for help) by checking whether the message came from the right place and right sender.

Even if the configuration of these protocols, technologies and methods may seem complex, we still advise companies and institutions to look into deploying them to reduce the risk of loss through phishing and malware. These protections will not eradicate those threats but they will make life much more difficult for attackers.