5. DATA GOVERNANCE: SECURITY AND PRIVACY

START WITH A STORY

Exposition
In 12th of May 2017, the highest level of ransomware attack occurred targeting all over the world. The Ransomware used exploit called EternalBlue, a vulnerability operated by the NSA and released to the public by ShadowBrokers.

Once a computer was infecteded with WannaCry, it encrypted all he data. The program put up a screen demanding a ransom in the form of virtual Bitcoin in order to gain back access, with the ransom increasing over time until the end of the countdown, when all the files would be destroyed.

Wannacry affected more than 200,000 systems from companies, government agencies and individuals in more than 150 countries. Major organisations such as the National Health Services (NHS)[1] in the United Kingdom and Renault-Nissan had to halt production in some areas as a result. A number of big businesses were also affected, including Telefonica, FedEx, Deutsche Bahn, Santander, and KPMG.

Why was this attack so potent?

- Firstly, the way it spread. The most common infection route of conventional Ransomware was by spreading via phishing e-mail and visiting a website. Ransomware was distributed as a mail to encourage users to click on email attachments or hack into a web server and disguised as an advertisement, so when a user visits the website, the user PC gets infected. However, WannaCry ransomware had characteristics of a worm, which is distributed autonomously through the network without any user action. Every Windows computer without patch was vulnerable to the infection.
- Secondly, unprotected operating systems. One of the biggest contributor was that a large number of computers did not have Microsoft's patch installed or ran versions of Windows for which there was no patch.

Lessons
Leaders failed to recognise that in order to deter and minimise the potential of cyber attacks, they need to ensure that their operating systems are constantly updated and patched across all networks.

EXPOSITION

1. DATA SECURITY

Experts warn that WannaCry was just the beginning, and the numbers confirm this view.

Among small business owners prevails the unfortunate misconception that hackers are interested only in attacking large enterprises. The fact is, hackers love SMEs. These smaller businesses tend to focus less on security and don't have the IT security budgets large enterprises have.
don't have the funds to pay for security analysts or inhouse IT.[2]

Types of threats

[1] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
[2] https://www.telegraph.co.uk/business/cybersecurity-for-small-business/fraud-prevention/

A data breach is an incident in which sensitive or otherwise protected information is accessed without authorisation. It can drain what meager resources SMEs do have and diminish consumer confidence. In short, lack of security can bankrupt you.

2. DATA PRIVACY

Why does Privacy matter?

1. Limit on Power. Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives. Personal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behavior. It can be used as a tool to exercise control over us. And in the wrong hands, personal data can be used to cause us great harm.[3]

2 Freedoms. Privacy is key to freedom of thought and expression and helps protect our ability to associate with other people. A key component of freedom of association is the ability to do so with privacy if one chooses. Privacy is a critical component of a democratic society.

3. Rights to a Second Chance Many people are not static; they change and grow throughout their lives. There is a great value in the ability to have a second chance, to be able to move beyond a mistake, to be able to reinvent oneself. Privacy nurtures this ability. It allows people to grow and mature without being shackled with all the foolish things they might have done in the past

Data protection is different to data privacy

- Privacy is a complicated issue relating to rights and freedoms enshrined under law. Data protection is different to data privacy. Protection is about securing data against unauthorized access. Data privacy is about authorized access — who has it and who defines it. Data protection is essentially a technical issue, whereas data privacy is a legal one.
- Technology alone cannot ensure the privacy of personal data. Most privacy protection protocols are still vulnerable to authorized individuals who might access the data. The burden on these authorized individuals is, above all, about privacy law, not technology.

GDPR

- GDPR is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.[4]
- It's objective is to hold companies accountable for safeguarding the personal data increasingly swept up in today's digital world
- It falls to national regulators—in Britain, the Information Commissioner's Office—to enforce the rules for companies within their jurisdiction.
- Penalties: Under GDPR, regulators can fine a company as much as 4% of annual sales, though most fines so far have been far smaller, typically less than $1 million.

Personal data shall be:

- processed lawfully, fairly and in a transparent ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

[3] https://teachprivacy.com/10-reasons-privacy-matters/

[4] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- accurate and, where necessary, kept up to date (‘accuracy’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

British Airways case study

- Half a million passenger records were accessed in a cyberattack between 21st Aug and 5th Sept 2018. The company resolved the breach of its website and app on 6th Sept and the police were notified.
- The Information Commissioner’s Office (ICO) stated that a variety of information was compromised by poor security arrangements, including login, payment-card and travel booking details as well as name and address information.
- The airline will have to pay £183.39 million ($230 million) to the ICO for failing to protect its customers' data, the biggest penalty initiated by national-privacy regulators across the EU since the enactment of GDPR.[5]

3. DATA ETHICS

The power of data is so large and can have such a big effect on our lives that we should imagine data not as Is and Os but as a digital soul. The concept of a ‘digital soul’ was described as the electronic representation of yourself. Creating a model for ownership and control of this idea is the big challenge to companies that hold data, as well as individuals and regulators

Lessig’s Pathetic dot

The pathetic dot theory or the New Chicago School theory was introduced by Lawrence Lessig in a 1998 article and popularized in his 1999 book, *Code and Other Laws of Cyberspace*. It is a socioeconomic theory of regulation.[6] It discusses how lives of individuals (the pathetic dots in questions) are regulated by four forces: the law, social norms, the market, and architecture (technical infrastructure).

The theory highlights how computer code is just one of the regulatory modalities that can alter behaviour, and so understanding other mechanisms such as the law, norms and ethics is vital for building technologies that do not result in unwanted behaviour.

Data ethics is about going beyond the legislation and understanding how markets, norms and code interact to ensure we are ethical in our use of individual’s data. We must go beyond compliance, to using data in the best possible way for everyone involved.

Three Big themes

Consent. Consent is what many people discuss when they think of technology ethics.
Under the GDPR the requirements for consent have been strengthened to require a positive and unambiguous action to ‘opt in’. It is no longer a one-off decision but an on-going issue to be carefully

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

[6] https://en.wikipedia.org/wiki/Pathetic_dot_theory

monitored. Individuals may withdraw their consent at any time without penalty. The mechanisms for withdrawing consent should be as easy as those for giving consent. Individuals must be given a genuine choice about whether or not they consent. If they do not have a choice then consent will not be deemed to have been freely given and will not be valid.

Data sharing. Strong ethical and risk mitigation practices preclude sharing data without the consent of the people who disclose it. They also preclude sharing data with parties to whom access has not been granted. But the effective use of data demands that it should be shared—and particularly so in the digital business era, with a growing platform economy. More and more organizations are partnering to create new offerings and even new industries. These collaborations necessitate widespread and constant data sharing, bringing new and difficult to- predict risks. These risks are compounded by the fact that once data sets reach a large enough size, anonymity is a myth.[6] And when additional data sets are aggregated, individuals can be identified with relative ease.[7],[8] Addressing the issues and damage associated with sharing data, Figure 5 shows a set of guiding principles that can be put in place to mitigate risk.[9] (Accenture [7])

Algorithmic accountability and bias. Ways in which classification algorithms can be adapted or evaluated to mitigate potential bias or transparency problems. For years, dozens of reports by organizations such as ProPublica have been exposing the scale of algorithmic discrimination in criminal risk assessment, predictive policing, credit lending, hiring, and more.
Bias may be a human problem, but *amplification* of bias is a technical problem — a mathematically explainable and controllable byproduct of the way models are trained.
Just because an algorithm is fair does not mean it is used fairly . Practitioners should take action by carefully reviewing algorithmic approaches to mitigating bias. It is our responsibility to critically interrogate who benefits from these technologies at whose costs, and to be vocal about how our models should or should not be used.

Examples of algorithmic bias
Facial recognition software is increasingly being used in law enforcement – and is another potential source of both race and gender bias. In February this year, Joy Buolamwini at the Massachusetts Institute of Technology found that three of the latest gender-recognition AIs, from IBM Microsoft and Chinese company Megvii, could correctly identify a person's gender from a photograph 99 per cent of the time – but only for white men. For dark-skinned women, accuracy dropped to just 35 per cent. That increases the risk of false identification of women and minorities. Again, it's probably down to the data on which the algorithms are trained: if it contains way more white men than black women, it will be better at identifying white men. IBM quickly announced that it had retrained its system on a new data set, and Microsoft said it has taken steps to improve accuracy.
Source: New Scientist : https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/#ixzz5vqEWBlh2

4. INFORMATION GOVERNANCE

Data breaches are serious, and customers themselves demand ever better attention to data ethics, so we need to take data governance seriously. Companies need an emergency plan, but prevention is better than cure.

There is no one-size-fits-all solution.

[7] https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf

Definition: "… specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information." (Logan, 2010). In order words, it comprises a set of rules and guidance to how data or information is handled within an organization. (Quoted in Rising, Kristensen, Tjerrild-Hansen, 2014[8])

Goals

1. maximize the value of information to the organization by ensuring that information is reliable, secure, and accessible for decision making
2. protect information so that its value to the organization is not diminished through technology or human error, loss of timely access, inappropriate use, or misadventure.

Why is it information governance and not data governance?
"Simply put, data refers to raw, unorganized facts. Think of data as bundles of bulk entries gathered and stored without context. Once context has been attributed to the data by stringing two or more pieces together in a meaningful way, it becomes information." Lebanthal

4 Risk Assessment

A risk assessment helps you understand the areas you need to protect, those where you could be most vulnerable and potential worst-case scenarios. Start by auditing the data and information you hold that is most valuable. Then look at how you store this data, who has access to it and how it's protected by technology and processes, to understand where you could be most at risk. If you're not confident carrying out a risk assessment, then you might want to consider hiring an expert to do this for you.

An effective response plan should include the following elements:

- Your legal response: You need to outline how you'll handle the legal aspects of the breach, for example informing the Information Commissioner's Office (ICO) of the issue and defending your business against any claims of negligence.
- Handling media queries: Your business could be the focus of media attention following a breach, so be ready to handle all external communications about what happened and how you're handling it. You are likely to need professional PR expertise to do this effectively.
- Finding out what happened: You'll also need to have IT forensics experts on hand to find out what caused the breach, with a view to rectifying the problem quickly and ensure it doesn't happen again.
- Informing customers: Depending on your customer-base and the scale of the breach, you could have a lot of unpleasant phone calls to make! You'll need to be ready with a way to handle this communication efficiently.

NOTE ON
Cyber Insurance

If you're facing the repercussions of a data breach, your final line of defence is a watertight and specialist cyber insurance policy. Covering you for breach of data protection laws (where insurable by law) and your liability for handling data, it can also provide cover for extortion, system rectification costs, plus PR expenses and financial loss due to system downtime.

Some key aspects to look out for include:

- The Information Commissioner's Office (ICO) can give fines of up to £500,000 for breach of the Data Protection Act. The Digital Risks cyber insurance policy will cover notification costs,

[8] https://web.stanford.edu/class/msande238/projects/2014/GainIT.pdf

legal fees defending regulatory action, and in some cases the penalty itself (where this can legally be insured).

- Cover for your out-of-pocket expenses, which could include system repair costs, lost income while the system is down, or even ransom payments to hackers.
- Cover for your website, blogs and social media, for copyright or trademark infringement, or defamation etc.

GENERATION DATA

USING DATA FOR PROFIT

Case Studies

Facebook Social Security Case Study

CYBERNET SECURITY CENTER UNDER THE MINISTRY OF DEFENSE

FACEBOOK SOCIAL SECURITY

Why might your personal account be useful?

• For personal information about you:

o Contacts; o pictures; o other personal information (when you went, where you went, where you live, paid, work, hobbies, hobbies, etc.);

• For information about the people you are communicating with;

• Fake page ratings, comments, etc.;

• For Facebook groups and pages administered by your account.

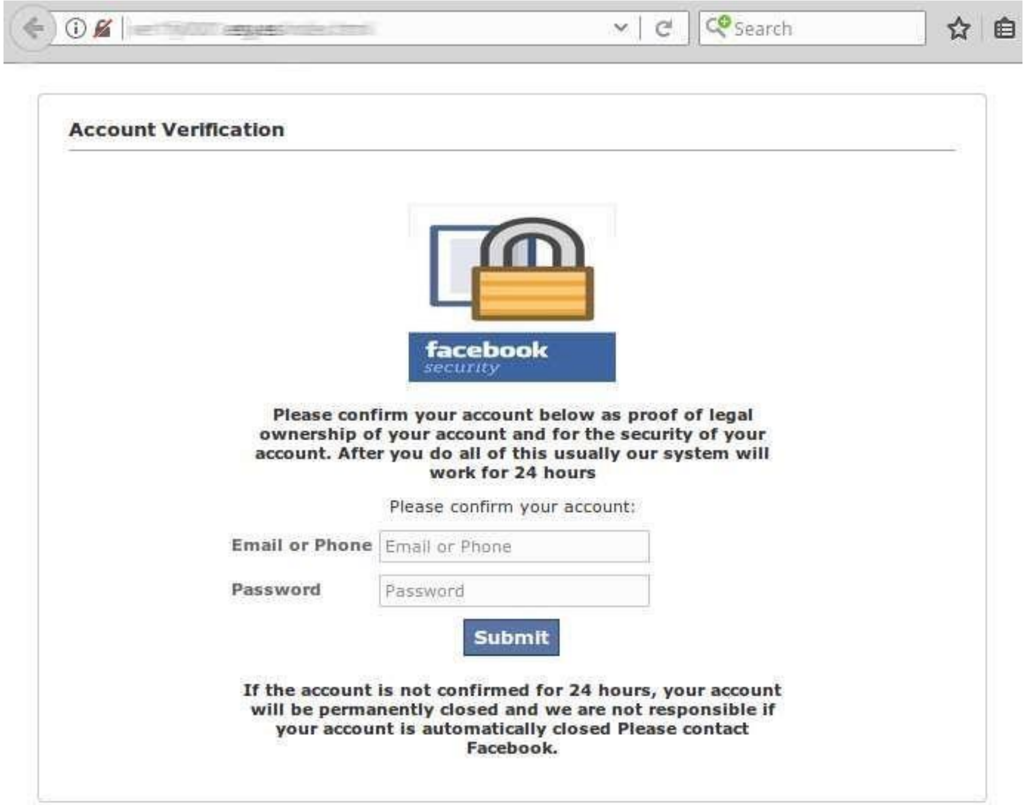
Particular attention is paid to Facebook groups, pages and individuals - especially those who have a significant number of followers. Stolen Facebook pages and accounts are maliciously sold to third parties, exploited for advertising and other purposes.

How are Facebook accounts hijacked?

• Mostly stolen password protected accounts;

• Login details come from other sources (email, other online accounts); • Login credentials are collected on public devices and publicly available free wireless networks (free wifi);

• Login stolen through social engineering (by sending fake emails with links to Facebook phishing)



Account Verification

facebook
security

Please confirm your account below as proof of legal ownership of your account and for the security of your account. After you do all of this usually our system will work for 24 hours

Please confirm your account:

Email or Phone: Email or Phone

Password: Password

Submit

If the account is not confirmed for 24 hours, your account will be permanently closed and we are not responsible if your account is automatically closed Please contact Facebook.

Figure 1. An example of social engineering is page forgery

Liability for Unauthorized Login to Your Facebook Account.

Liability for such activities is described in Articles 198 1 (1) and 198 2 (1) of the Criminal Code of the Republic of Lithuania.

Article 198 1. Illegal access to information system

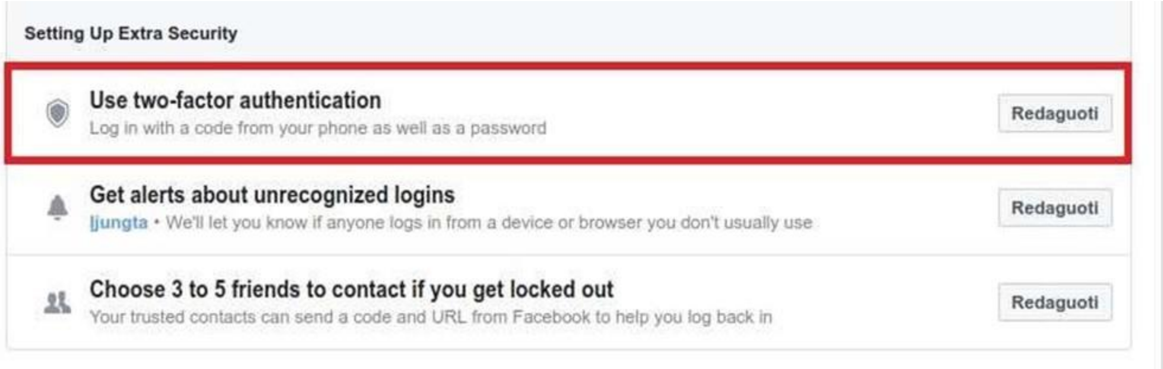
Whoever illegally accessed the information system or part of it in breach information system security measures punishable by public works or fines, or arrest, or imprisonment for up to two years.

Article 198 2. Unauthorized disposal of devices, software, passwords, codes, and other data

Anyone who, for criminal purposes or otherwise, has produced, transported, imported, sold, made available or otherwise distributed, acquired or possessed devices or software directly intended or adapted for committing crimes, as well as passwords, codes or other similar data for logging on to an information system or part thereof, punishable by public works, or by fine, or by arrest or imprisonment for up to three years.

Recommendations on how to prevent burglaries

- Use a secure password (it is recommended that the password be at least 9 characters, including uppercase and lowercase letters, numbers, and punctuation);
- Don't divulge your password to anyone;
- Don't use the same password you use for other accounts;
- Don't sign in to your account on public devices;
- Avoid placing excessive information on social networks;
- Use two-factor authentication (Settings ➔ Security and logins)



Setting Up Extra Security

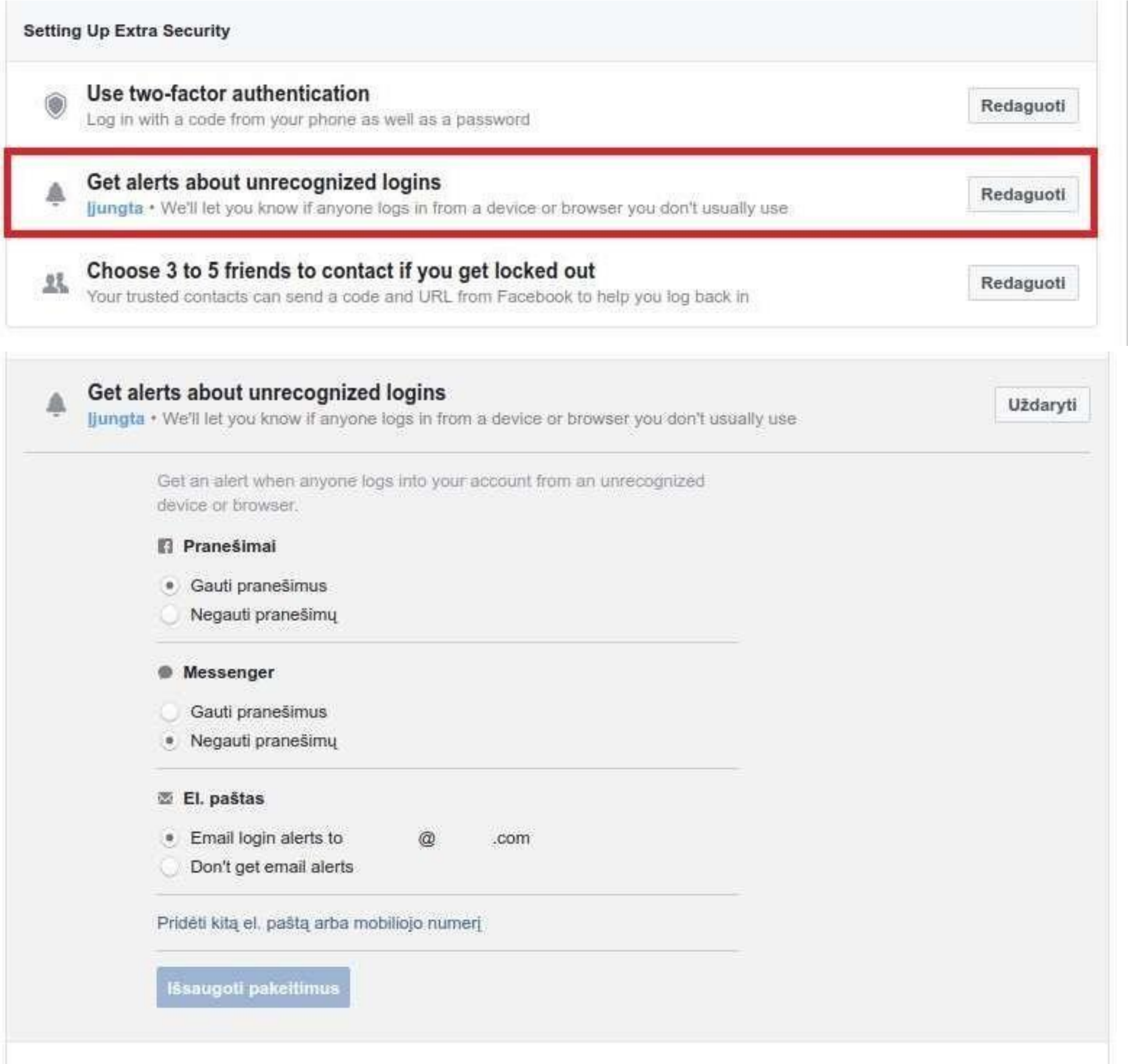
Use two-factor authentication
Log in with a code from your phone as well as a password

Get alerts about unrecognized logins
ljungta • We'll let you know if anyone logs in from a device or browser you don't usually use

Choose 3 to 5 friends to contact if you get locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in

Figure 2. Set up two-factor authentication

- Set up to receive email. Notify you of unsuccessful logins to your account (Settings ➔ Security and logins).



Setting Up Extra Security

Use two-factor authentication
Log in with a code from your phone as well as a password — Redaguoti

Get alerts about unrecognized logins
Įjungta • We'll let you know if anyone logs in from a device or browser you don't usually use — Redaguoti

Choose 3 to 5 friends to contact if you get locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in — Redaguoti

Get alerts about unrecognized logins
Įjungta • We'll let you know if anyone logs in from a device or browser you don't usually use — Uždaryti

Get an alert when anyone logs into your account from an unrecognized device or browser.

Pranešimai

- ● Gauti pranešimus
- ○ Negauti pranešimų

Messenger

- ○ Gauti pranešimus
- ● Negauti pranešimų

El. paštas

- ● Email login alerts to @ .com
- ○ Don't get email alerts

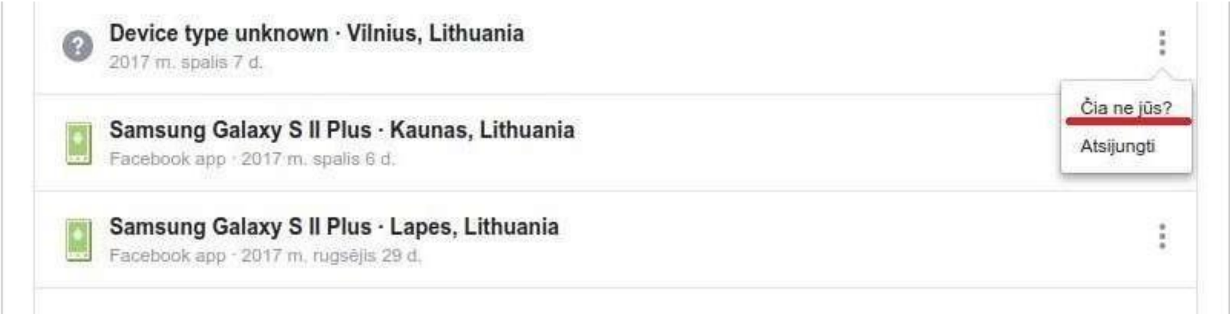
Pridėti kitą el. paštą arba mobiliojo numerį

Išsaugoti pakeitimus

Figure 3. Notifications of failed login to your account

What should I do if I notice suspicious activity or lose my Facebook account?
If you suspect that third parties have accessed your account:

- Change your password as soon as possible;
- Check for suspicious connections (Settings ➔ Security and Connections), disconnect the following devices when noticed:



Device type unknown · Vilnius, Lithuania
2017 m. spalis 7 d.

Samsung Galaxy S II Plus · Kaunas, Lithuania
Facebook app · 2017 m. spalis 6 d.

Samsung Galaxy S II Plus · Lapes, Lithuania
Facebook app · 2017 m. rugsėjis 29 d.

Figure 4 The devices that signed in to your account

- If you are unable to sign in to your account, try to recover it using your email;
- You can report a lost account - https://www.facebook.com/hacked
- If you fail to recover your account yourself, you can contact law enforcement.

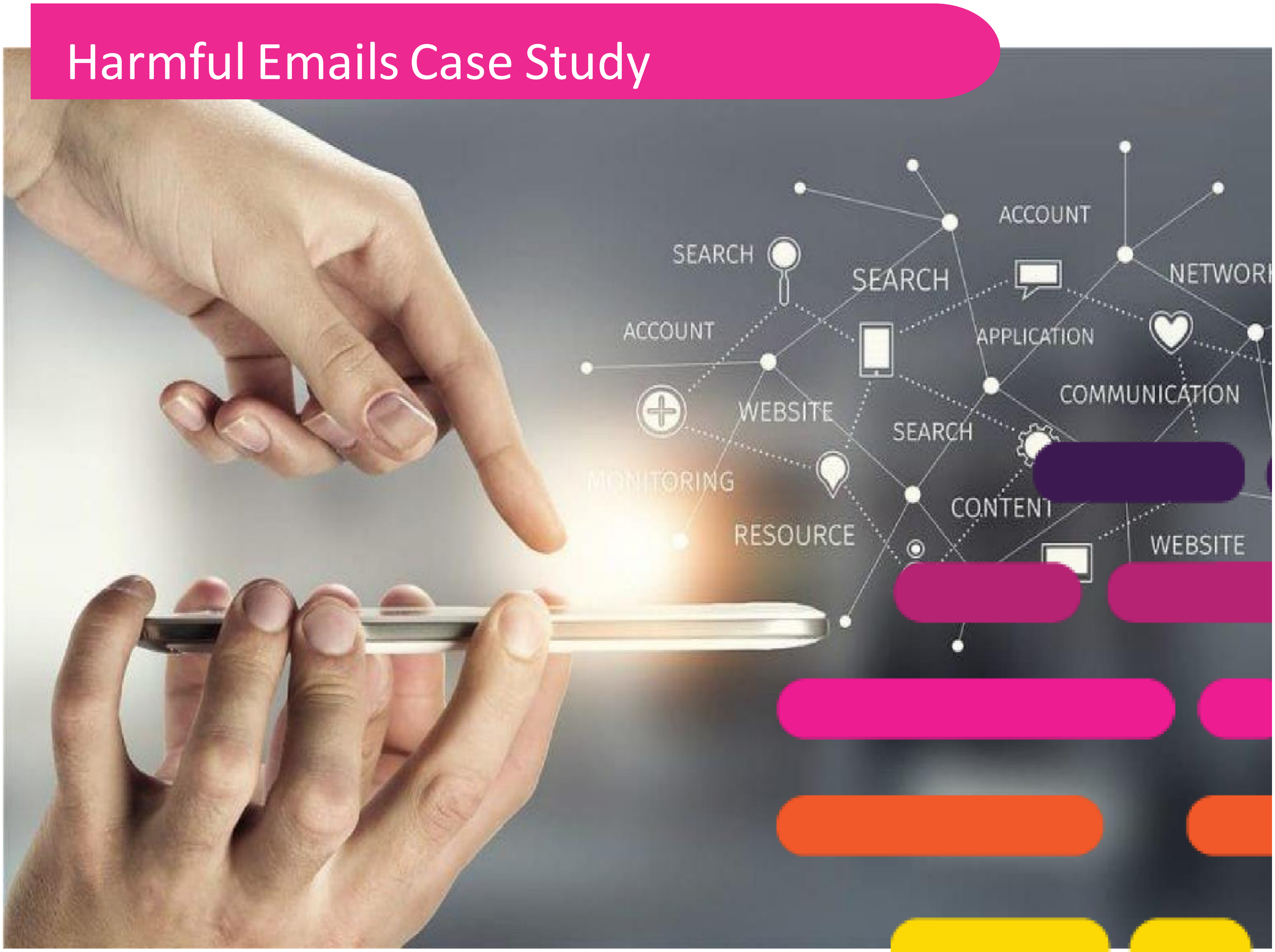
[Key Words: facebook, account, private data, social security, notification].

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

GENERATION DATA

USING DATA FOR PROFIT

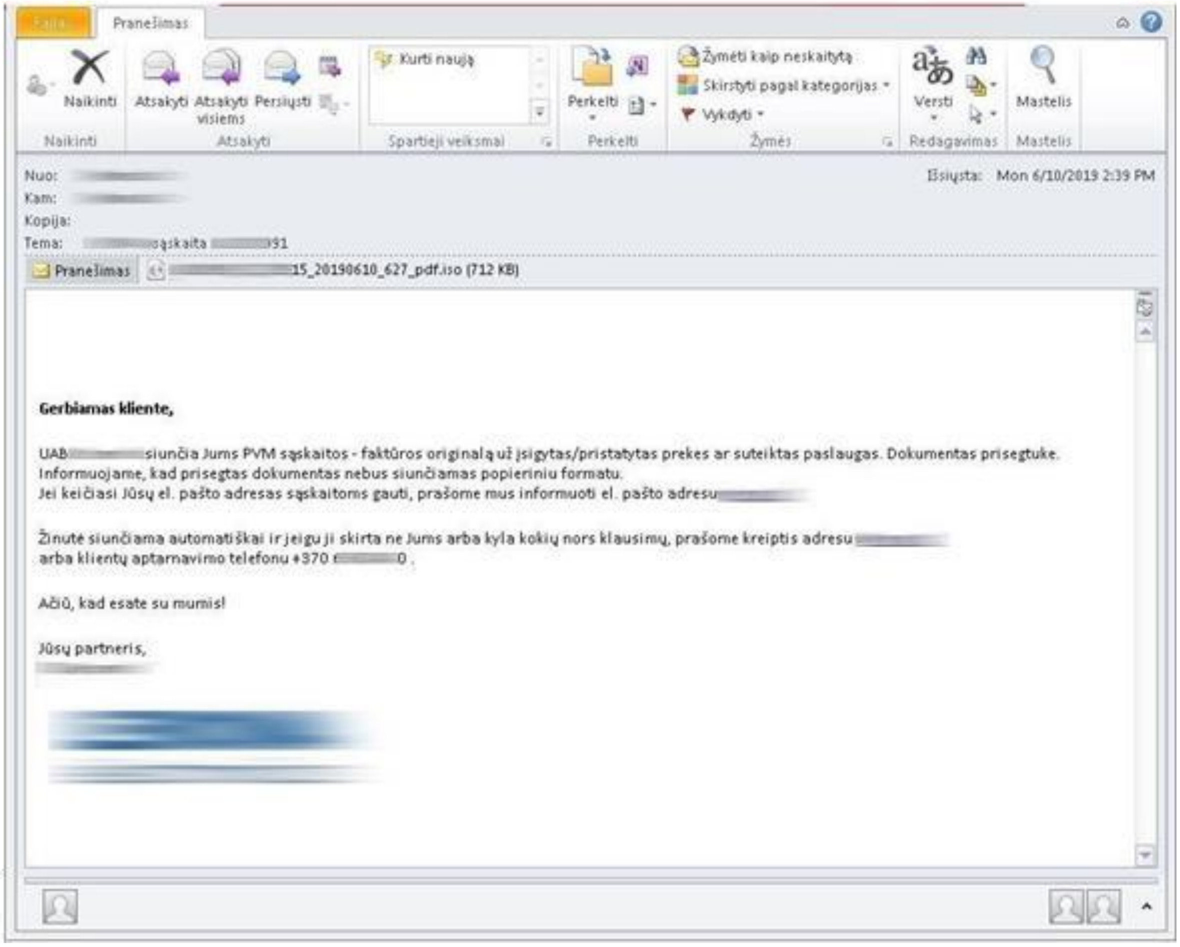
Harmful Emails Case Study



CYBERNET SECURITY CENTER UNDER THE MINISTRY OF DEFENSE

SENDING TO E-MAILED COMPANIES IN LITHUANIA LETTERS WITH HARMFUL SOFTWARE CODE

National Cyber Security Center under the Ministry of National Defense (NKSC) informs that in Lithuania are spreading emails with malicious code. In recent days NKSC records cases of falsification of e-mails of well-known Lithuanian and foreign companies, email addresses, their logos and contact information distribute malicious software code.



Nuo: [redacted]
Kam: [redacted]
Kopija:
Tema: [redacted]sąskaita [redacted]91
Išsiųsta: Mon 6/10/2019 2:39 PM
[redacted]15_20190610_627_pdf.iso (712 KB)

Gerbiamas kliente,

UAB[redacted]siunčia Jums PVM sąskaitos - faktūros originalą už įsigytas/pristatytas prekes ar suteiktas paslaugas. Dokumentas prisegtuke.
Informuojame, kad prisegtas dokumentas nebus siunčiamas popieriniu formatu.
Jei keičiasi Jūsų el. pašto adresas sąskaitoms gauti, prašome mus informuoti el. pašto adresu[redacted]

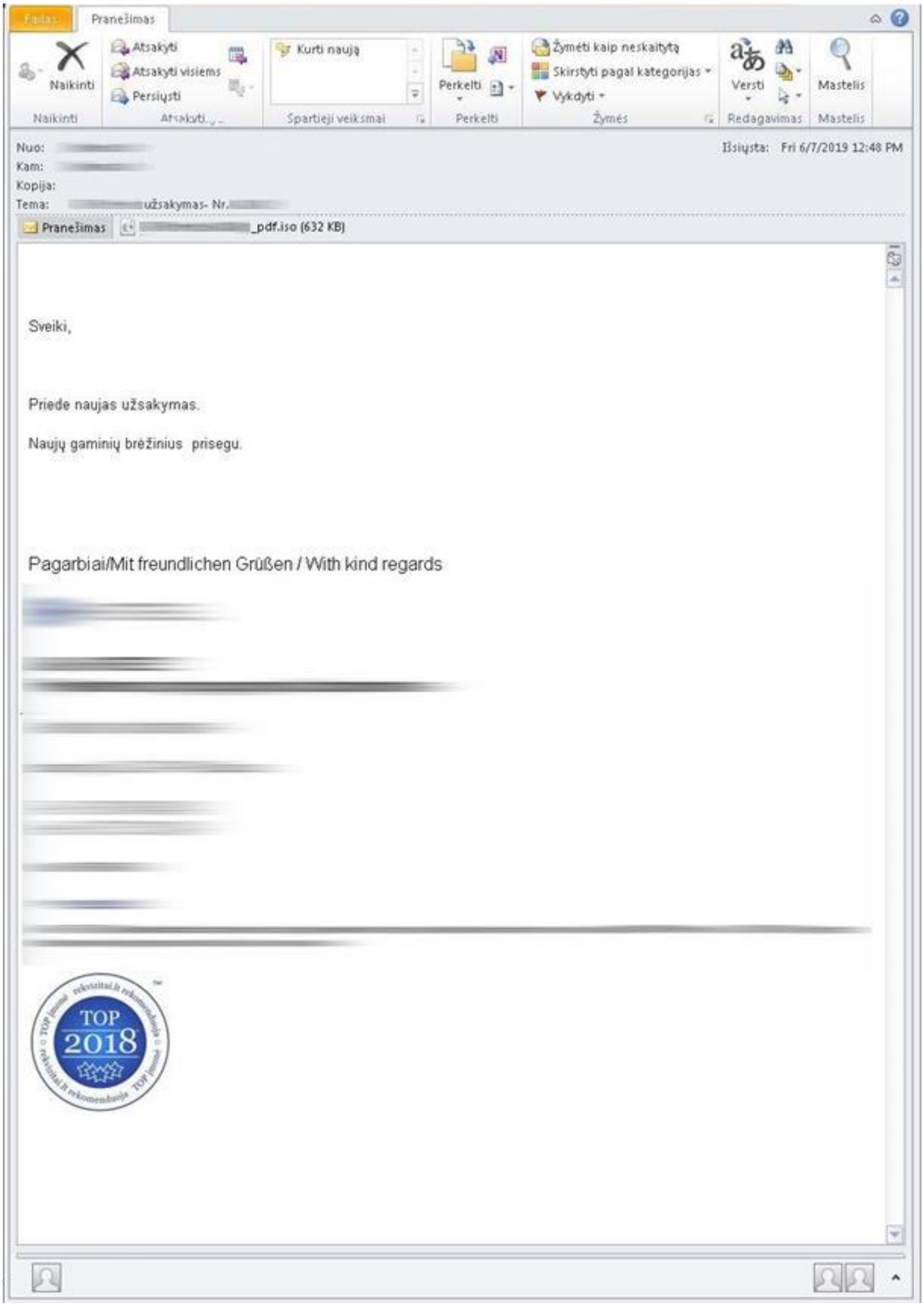
Žinutė siunčiama automatiškai ir jeigu ji skirta ne Jums arba kyla kokių nors klausimų, prašome kreiptis adresu[redacted]
arba klientų aptarnavimo telefonu +370 [redacted]0 .

Ačiū, kad esate su mumis!

Jūsų partneris,
[redacted]

[redacted]

Fig. 1. Fake email an example of a letter simulating a supplier



Nuo: [redacted]

Kam: [redacted]

Kopija:

Tema: [redacted]užsakymas- Nr.[redacted]

Išsiųsta: Fri 6/7/2019 12:48 PM

[redacted]_pdf.iso (632 KB)

Sveiki,

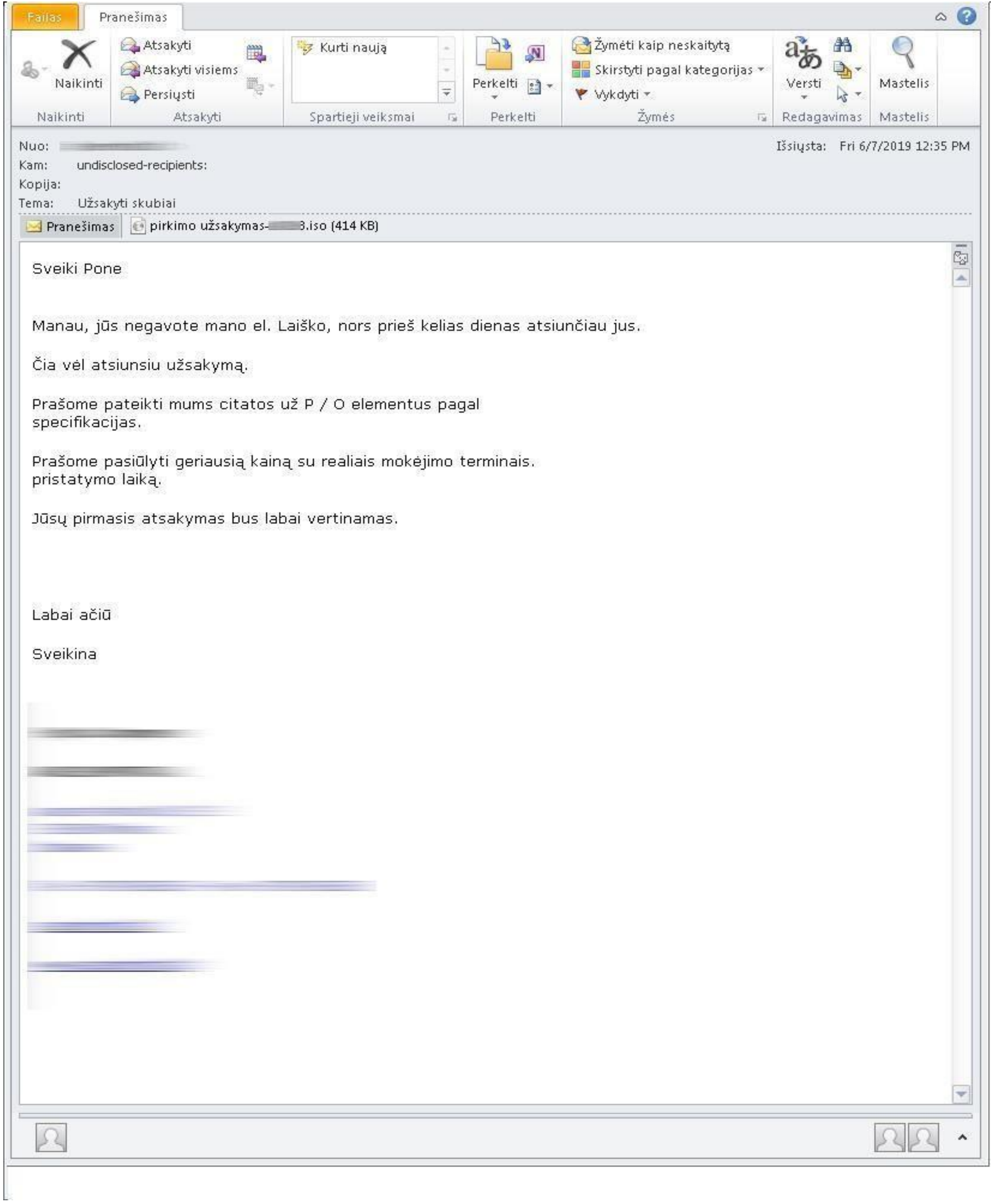
Priede naujas užsakymas.

Naujų gaminių brėžinius prisegu.

Pagarbiai/Mit freundlichen Grüßen / With kind regards

[redacted]

Fig. 2. Fake email an example of a letter simulating a supplier



Nuo: [redacted]

Kam: undisclosed-recipients:

Kopija:

Tema: Užsakyti skubiai

Išsiųsta: Fri 6/7/2019 12:35 PM

pirkimo užsakymas-[redacted]3.iso (414 KB)

Sveiki Pone

Manau, jūs negavote mano el. Laiško, nors prieš kelias dienas atsiunčiau jus.

Čia vėl atsiunsiu užsakymą.

Prašome pateikti mums citatos už P / O elementus pagal
specifikacijas.

Prašome pasiūlyti geriausią kainą su realiais mokėjimo terminais.
pristatymo laiką.

Jūsų pirmasis atsakymas bus labai vertinamas.

Labai ačiū

Sveikina

[redacted]

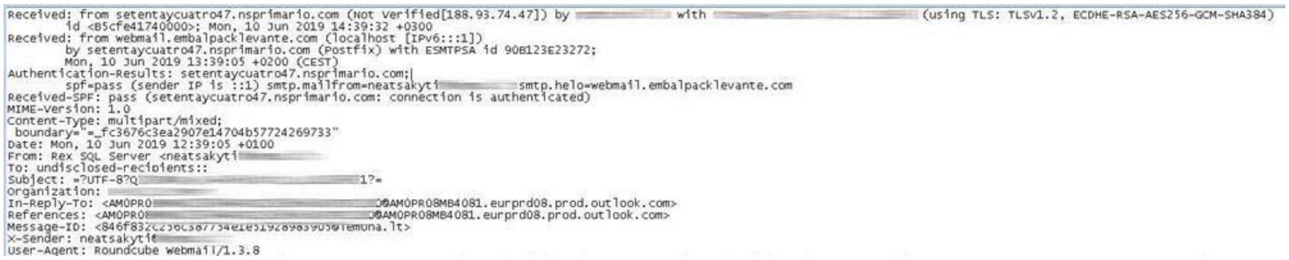
Fig. 3. Fake email an example of a letter simulating a supplier

The malicious code is hosted in * .iso files that are attached to email. Letter. The attached file contains the executable * .exe file. When the attachment is opened and the * .exe executable is executed, malicious software attempts to collect personal user information from the computer, retrieves the computer name, attempts to identify whether the computer can be accessed remotely (or Remote Desktop functionality), and sends information to a remote server. station and other intelligence activities.

The text of the letter is usually written in Lithuanian. The message seems realistic to the recipient, as it is sent from a known and trusted addressee, but is actually forged.

Recommendations

Check the headers of the message to see who is the real sender of the message (From field). When analysing a header, one should look at the first Received parameter from the bottom. This parameter will tell you from which server the email was sent. letter. If the From field is sender@imone.com, then the Received field should also show the address domain (domain) "imone.com". In the case of this scam, the Received field shows a completely different data from where the message was sent. See also: Fig. 4.



```
Received: from setentaycuatro47.nsprimario.com (Not Verified[188.93.74.47]) by [redacted] with [redacted] (using TLS: TLSv1.2, ECDHE-RSA-AES256-GCM-SHA384)
        id <B5cfe41740000>; Mon, 10 Jun 2019 14:39:32 +0300
Received: from webmail.embalpacklevante.com (localhost [IPv6:::1])
        by setentaycuatro47.nsprimario.com (Postfix) with ESMTPSA id 90B123E23272;
        Mon, 10 Jun 2019 13:39:05 +0200 (CEST)
Authentication-Results: setentaycuatro47.nsprimario.com;|
        spf=pass (sender IP is ::1) smtp.mailfrom=neatsakyti[redacted]smtp.helo=webmail.embalpacklevante.com
Received-SPF: pass (setentaycuatro47.nsprimario.com: connection is authenticated)
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="=_fc3676c3ea2907e14704b57724269733"
Date: Mon, 10 Jun 2019 12:39:05 +0100
From: Rex SQL Server <neatsakyti[redacted]
To: undisclosed-recipients::
Subject: =?UTF-8?Q[redacted]1?=
Organization: [redacted]
In-Reply-To: <AM0PR0[redacted]@AM0PR08MB4081.eurprd08.prod.outlook.com>
References: <AM0PR0[redacted]@AM0PR08MB4081.eurprd08.prod.outlook.com>
Message-ID: <846f8[redacted]temona.lt>
X-Sender: neatsakyti@[redacted]
User-Agent: Roundcube Webmail/1.3.8
```

Fig. 4. Fake Email true sender of the message

Depending on your email address for email clients, the ability to view headers varies. Please note that cybercriminals also regularly distribute other malicious code that exploits vulnerabilities in various software, and we recommend that you regularly update your antivirus, operating system, and other software you use.

To help prevent spam, we recommend that you enable and properly configure SPF (Sender Policy Framework) functionality in order to spam email contacts. This feature should be used with extra caution, as incorrect settings may cause some messages to be delivered to their recipients.

As a reminder, the key is to be constantly attentive and critical of incoming mail.

[Key Words: fake email, malicious software code, spam].

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.