Security Awareness

AGENDA

- Why Security Awareness is Essential?
- What is Security Awareness?
- What is the challenges?
- How do we start?
- Topics Covered

WHY SECURITY AWARENESS IS ESSENTIAL?

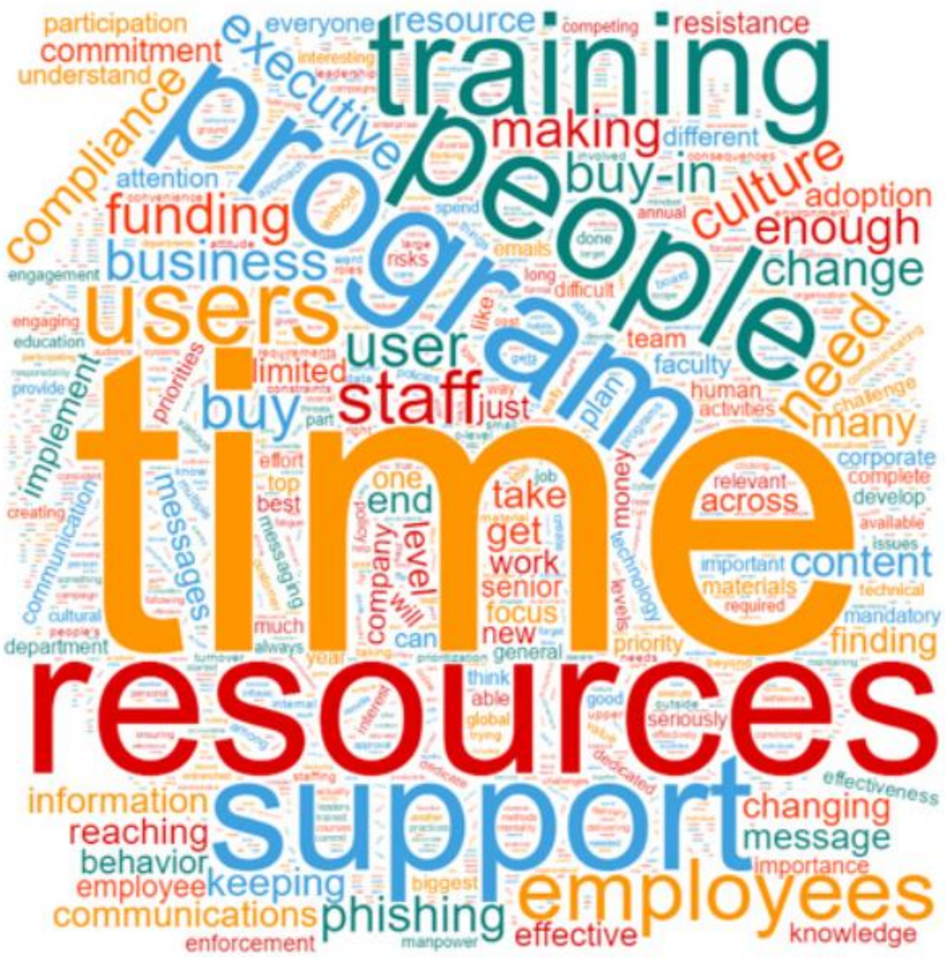
Human error causes alarming rise of 93% of data breaches globally

Infysec Solutions Private Limited

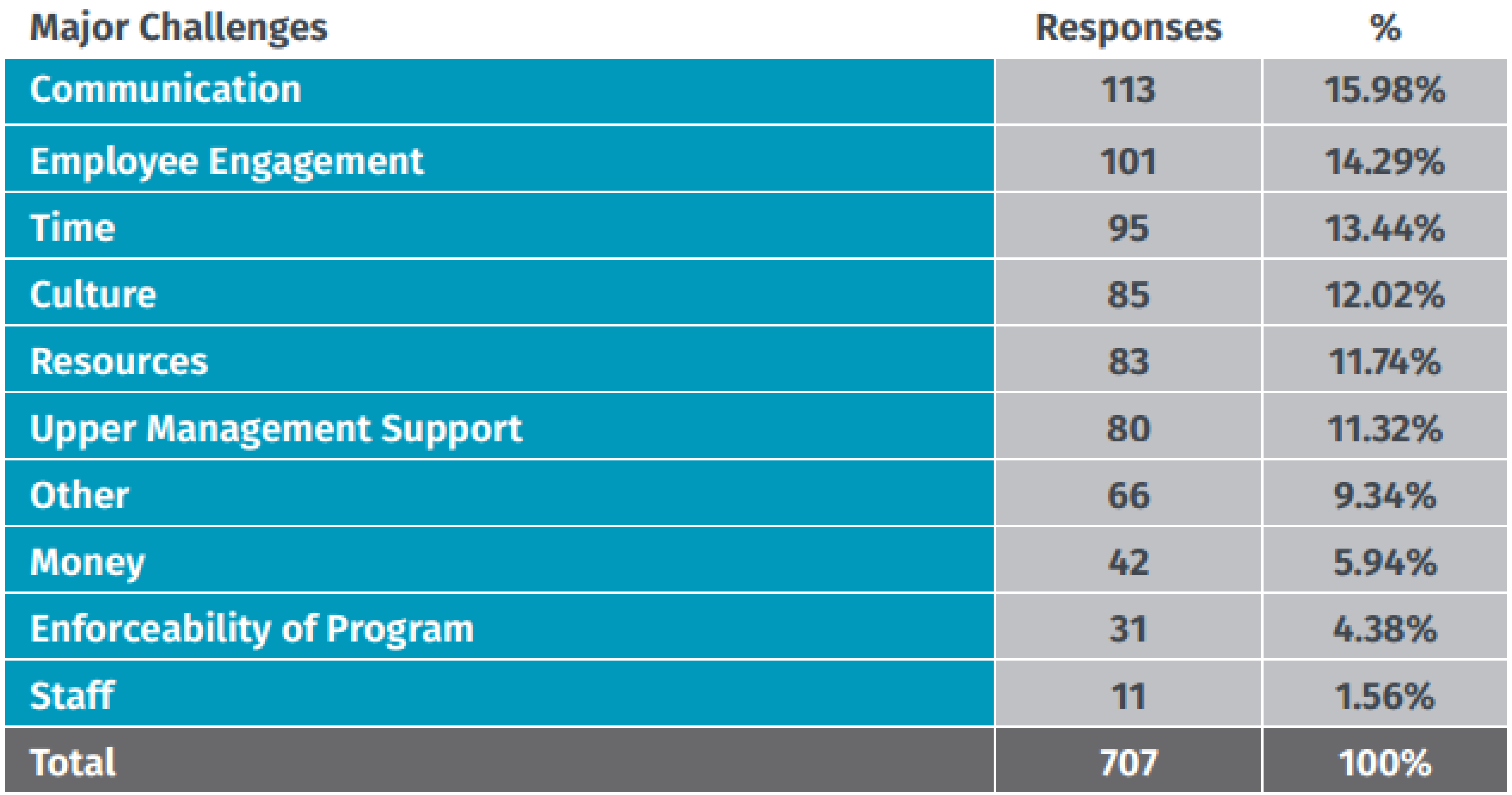
WHAT IS SECURITY AWARENESS?

- The knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.
- The advantage of knowing what types of security issues and incidents employees may face in the day-to-day routine of their corporate function

WHAT IS THE CHALLENGE?

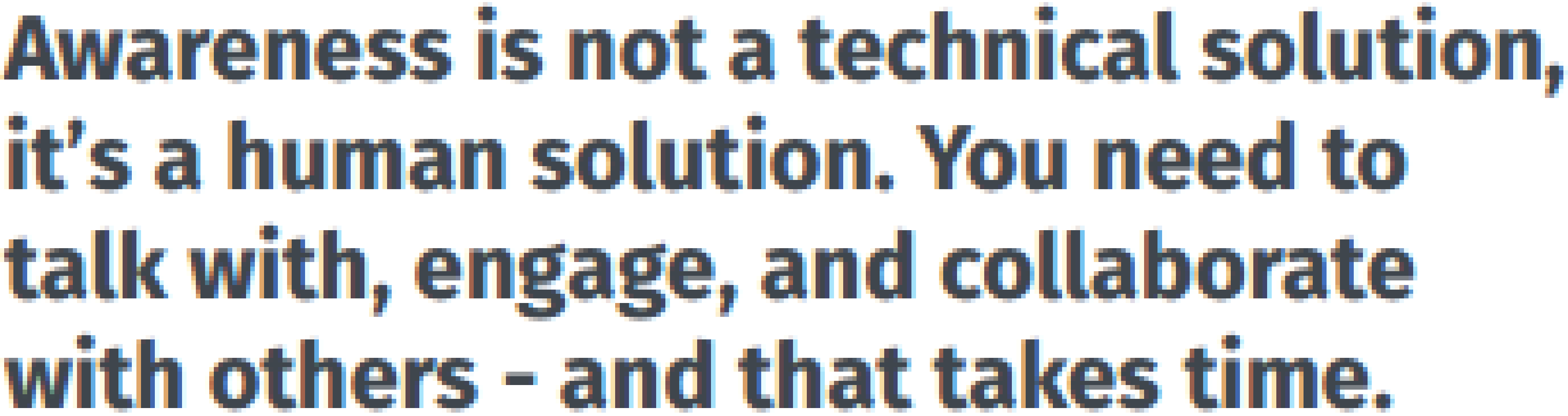


WHAT IS THE CHALLENGE?



Major Challenges	Responses	%
Communication	113	15.98%
Employee Engagement	101	14.29%
Time	95	13.44%
Culture	85	12.02%
Resources	83	11.74%
Upper Management Support	80	11.32%
Other	66	9.34%
Money	42	5.94%
Enforceability of Program	31	4.38%
Staff	11	1.56%
Total	707	100%

WHAT IS THE CHALLENGE?



Awareness is not a technical solution, it's a human solution. You need to talk with, engage, and collaborate with others - and that takes time.

HOW DO WE START?

- Become aware
  - Know how to identify a potential issues
  - Use sound judgement
- Learn and practice good security habits
  - Incorporate secure practices into your everyday routine
  - Encourage others to do so as well
- Report anything unusual
  - Notify the appropriate contacts if you become aware of security incidents

TOPICS COVERED

- Avoiding Dangerous Attachments
- Avoiding Dangerous Links
- Phising
- Social Engineering
- Passwords
- Access Rights
- Protecting Against Ransomware

AVOIDING DANGEROUS ATTACHMENTS

AVOIDING DANGEROUS ATTACHMENTS

They can spread malicious software.

Attackers use methods to entice you to open malicious email attachments through fear, curiosity, and urgency. Once you open a malicious attachment, malicious software (malware) can be installed without your consent or knowledge.

AVOIDING DANGEROUS ATTACHMENTS

They can compromise your device’s security.

The malware can enable attackers to access, control, and record information stored on your device.

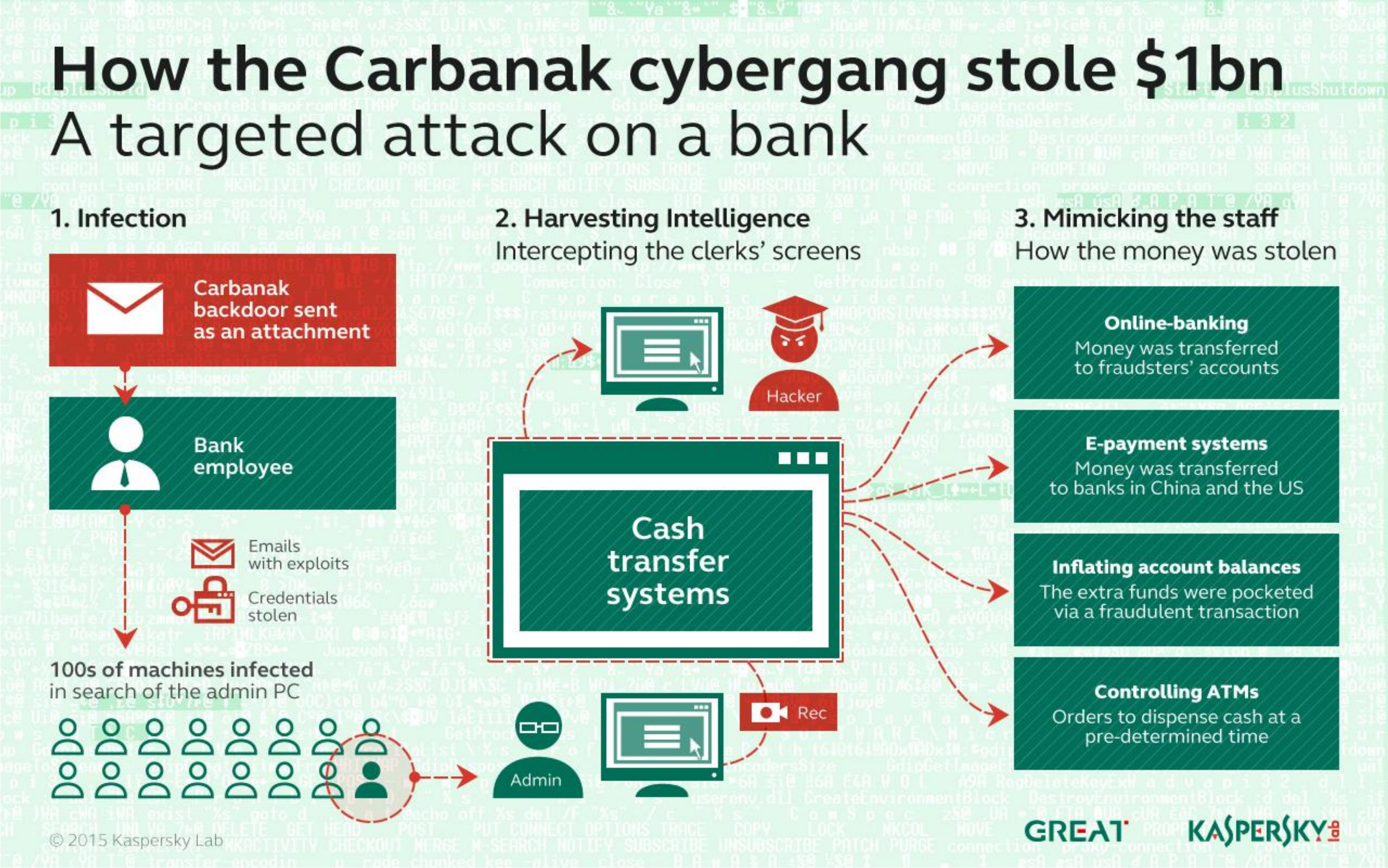
Some malware will even scan your device for email addresses and send the infected message to them.

AVOIDING DANGEROUS ATTACHMENTS

They can also compromise your employer's network.

Malware can quickly spread through your employer's networks via your device. This enables attackers to quickly acquire and leak sensitive or confidential data.

AVOIDING DANGEROUS ATTACHMENTS



How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected

in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Admin

Rec

3. Mimicking the staff

How the money was stolen

Online-banking

Money was transferred to fraudsters' accounts

E-payment systems

Money was transferred to banks in China and the US

Inflating account balances

The extra funds were pocketed via a fraudulent transaction

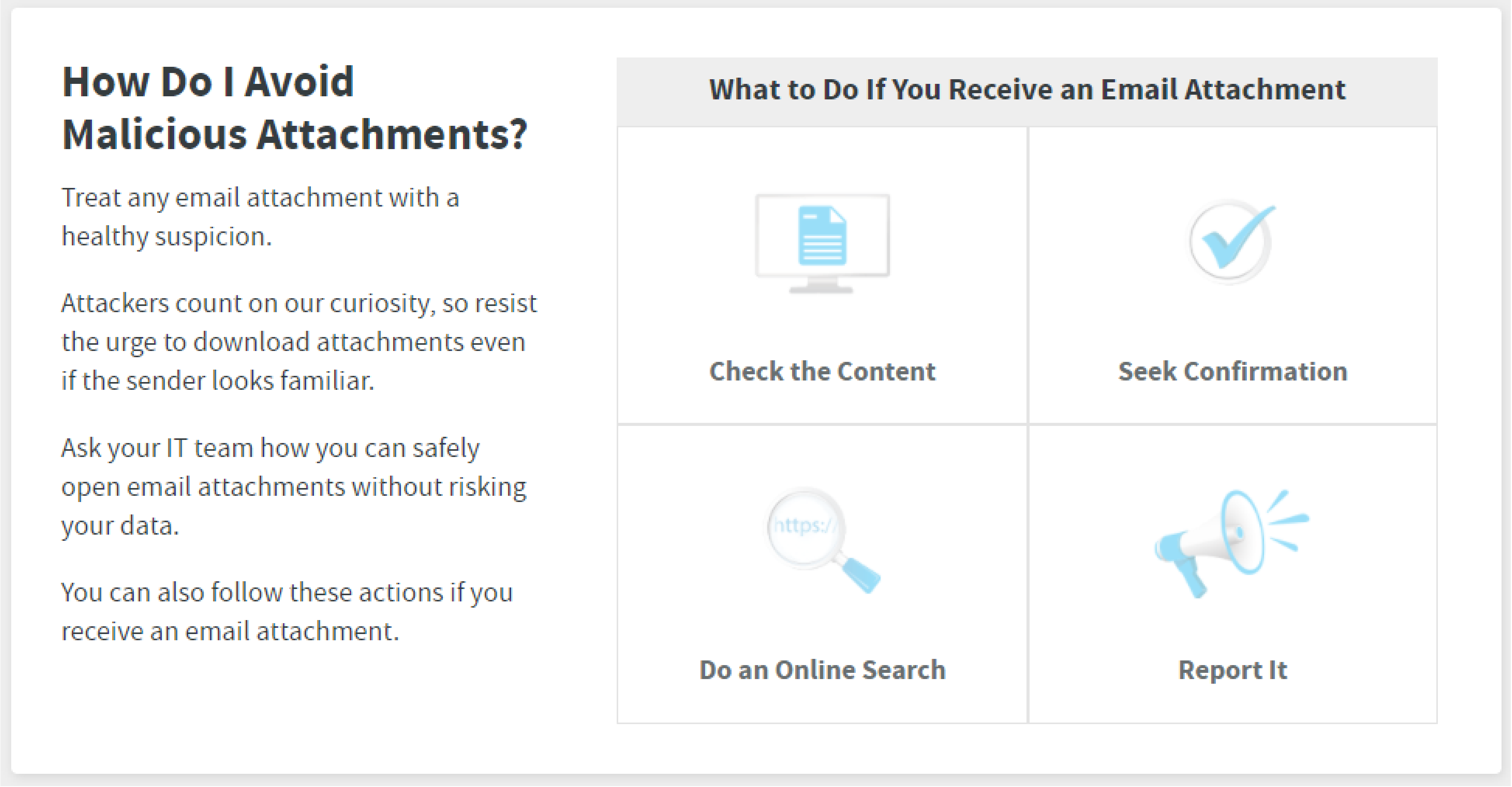
Controlling ATMs

Orders to dispense cash at a pre-determined time

© 2015 Kaspersky Lab

GREAT KASPERSKY lab

AVOIDING DANGEROUS ATTACHMENTS



How Do I Avoid Malicious Attachments?

Treat any email attachment with a healthy suspicion.

Attackers count on our curiosity, so resist the urge to download attachments even if the sender looks familiar.

Ask your IT team how you can safely open email attachments without risking your data.

You can also follow these actions if you receive an email attachment.

What to Do If You Receive an Email Attachment

Check the Content

Seek Confirmation

Do an Online Search

Report It

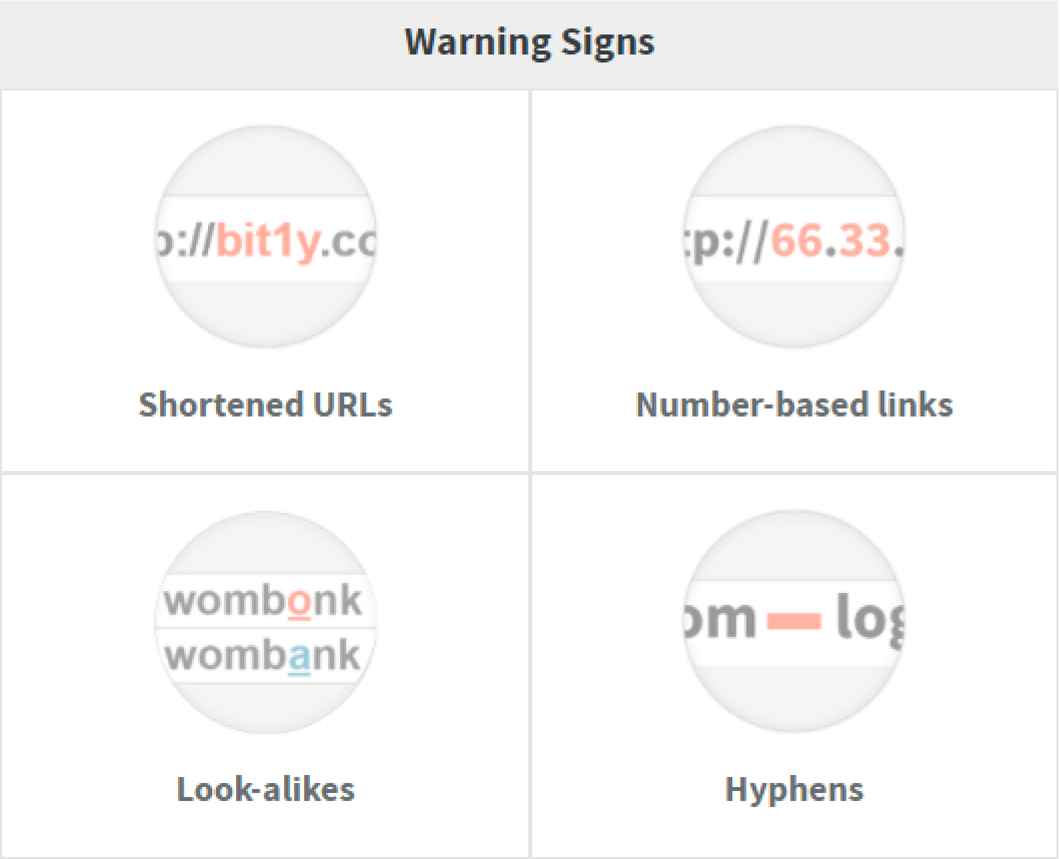
AVOIDING DANGEROUS LINKS

AVOIDING DANGEROUS LINKS

Attackers Manipulate URLs to Trick Users

Manipulating a URL goes beyond using the right words to trick you. Attackers will often change links in other ways to look like valid URLs.

If you see any of these warning signs in an email link, look, but don't click unless you are absolutely certain you can trust the URL.



Warning Signs

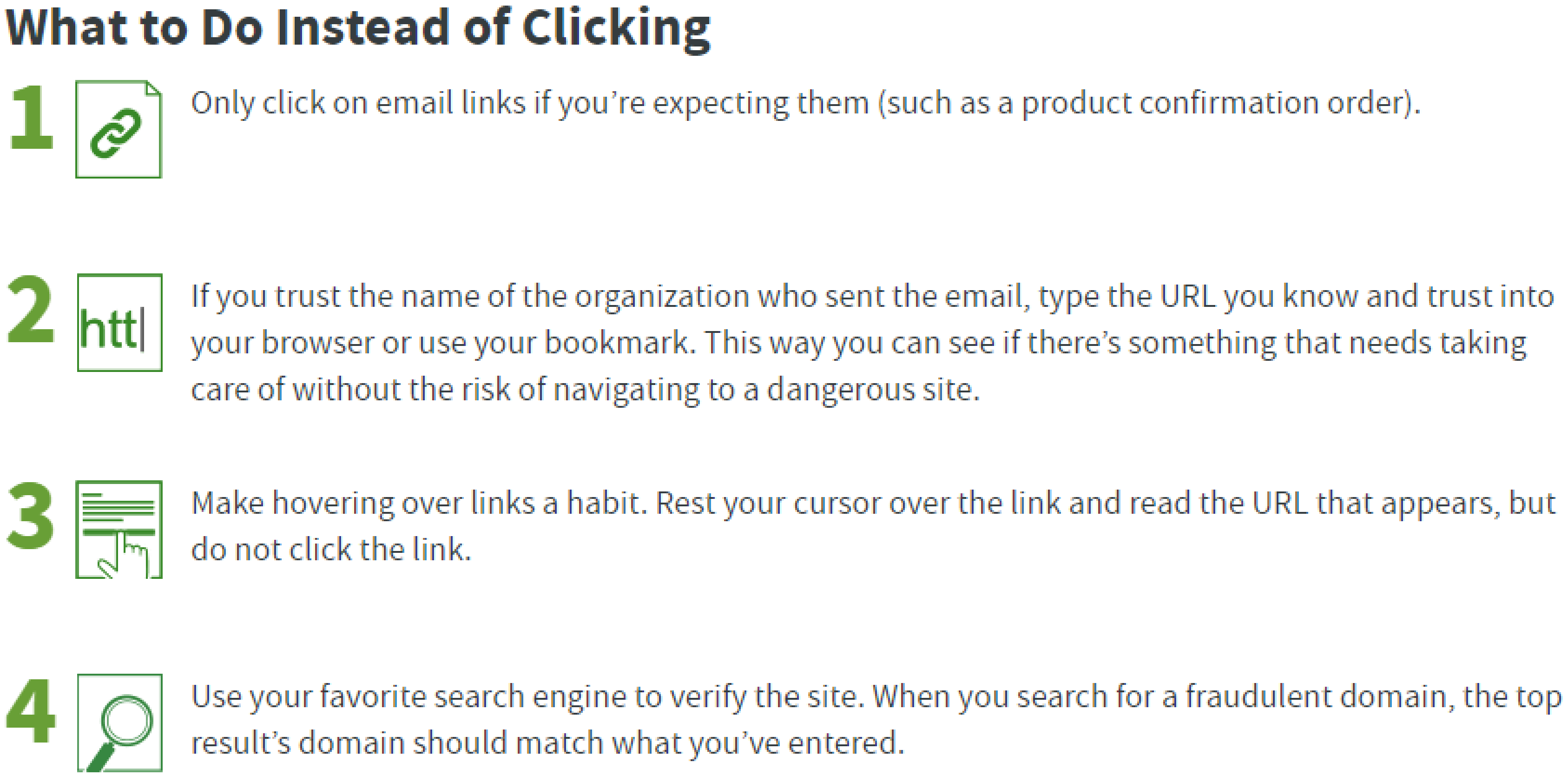
Shortened URLs

Number-based links

Look-alikes

Hyphens

AVOIDING DANGEROUS LINKS



What to Do Instead of Clicking

1 Only click on email links if you’re expecting them (such as a product confirmation order).

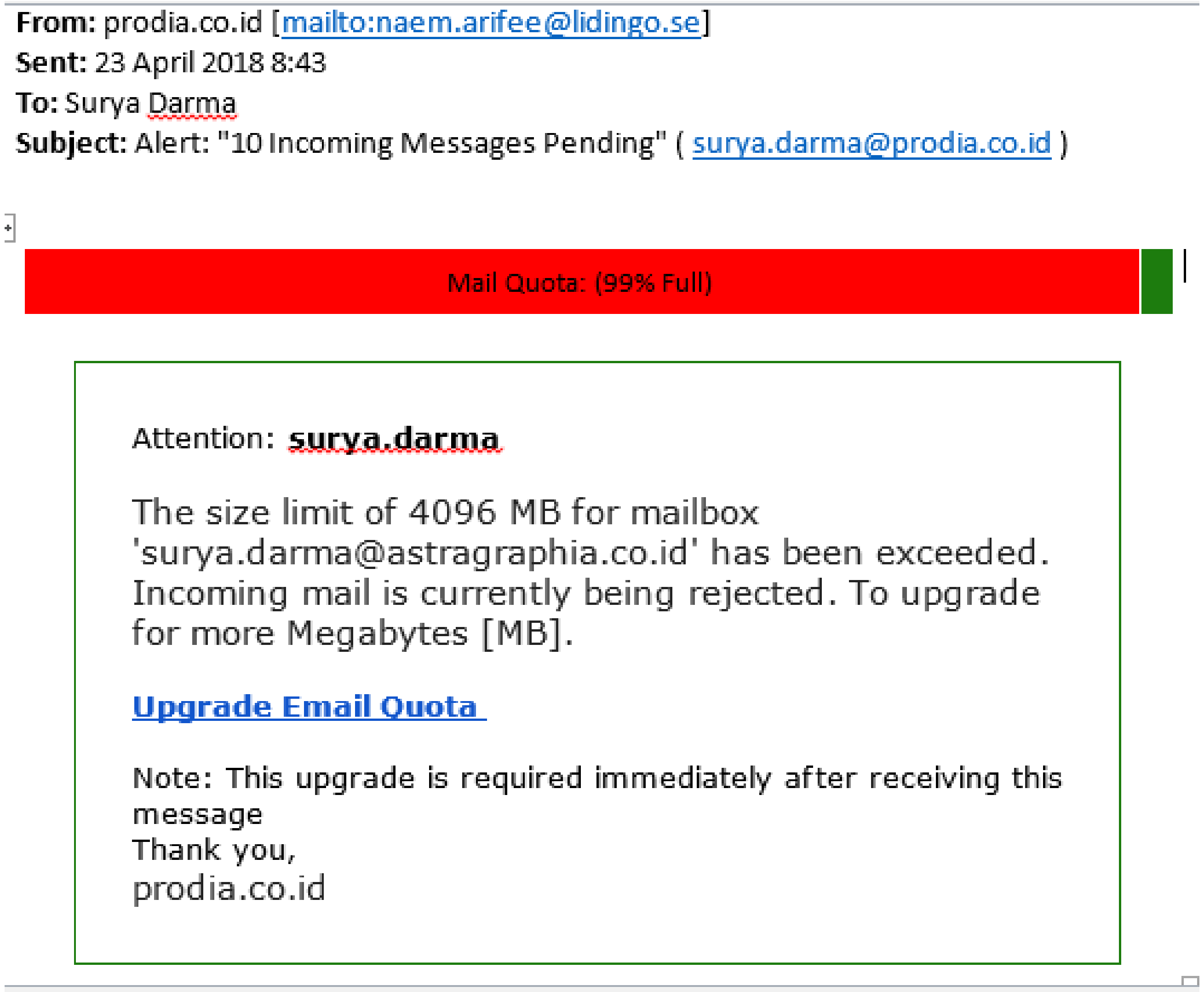
2 If you trust the name of the organization who sent the email, type the URL you know and trust into your browser or use your bookmark. This way you can see if there’s something that needs taking care of without the risk of navigating to a dangerous site.

3 Make hovering over links a habit. Rest your cursor over the link and read the URL that appears, but do not click the link.

4 Use your favorite search engine to verify the site. When you search for a fraudulent domain, the top result’s domain should match what you’ve entered.

PHISING

PHISING



From: prodia.co.id [mailto:naem.arifee@lidingo.se]
Sent: 23 April 2018 8:43
To: Surya Darma
Subject: Alert: "10 Incoming Messages Pending" (surya.darma@prodia.co.id)

Mail Quota: (99% Full)

Attention: **surya.darma**

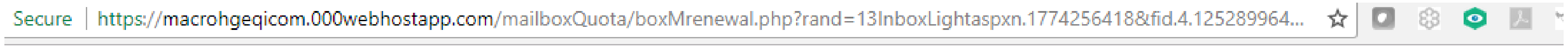
The size limit of 4096 MB for mailbox 'surya.darma@astragraphia.co.id' has been exceeded. Incoming mail is currently being rejected. To upgrade for more Megabytes [MB].

Upgrade Email Quota

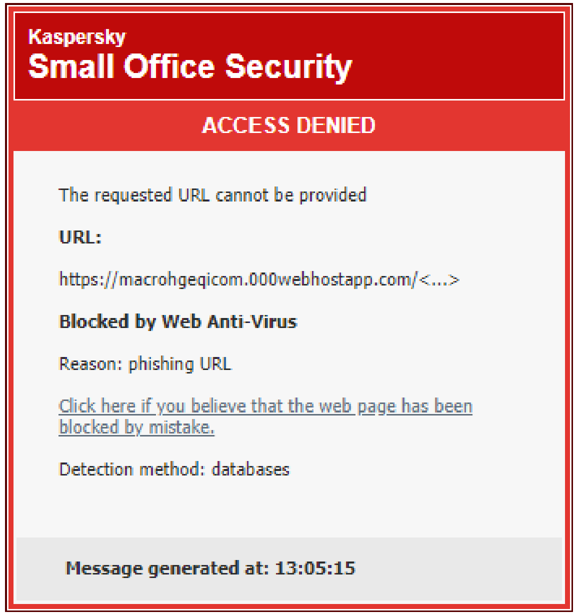
Note: This upgrade is required immediately after receiving this message
Thank you,
prodia.co.id

Click me..

PHISING



Secure | https://macrohgeqicom.000webhostapp.com/mailboxQuota/boxMrenewal.php?rand=13InboxLightaspxn.1774256418&fid.4.125289964...



Kaspersky
Small Office Security

ACCESS DENIED

The requested URL cannot be provided

URL:

https://macrohgeqicom.000webhostapp.com/<...>

Blocked by Web Anti-Virus

Reason: phishing URL

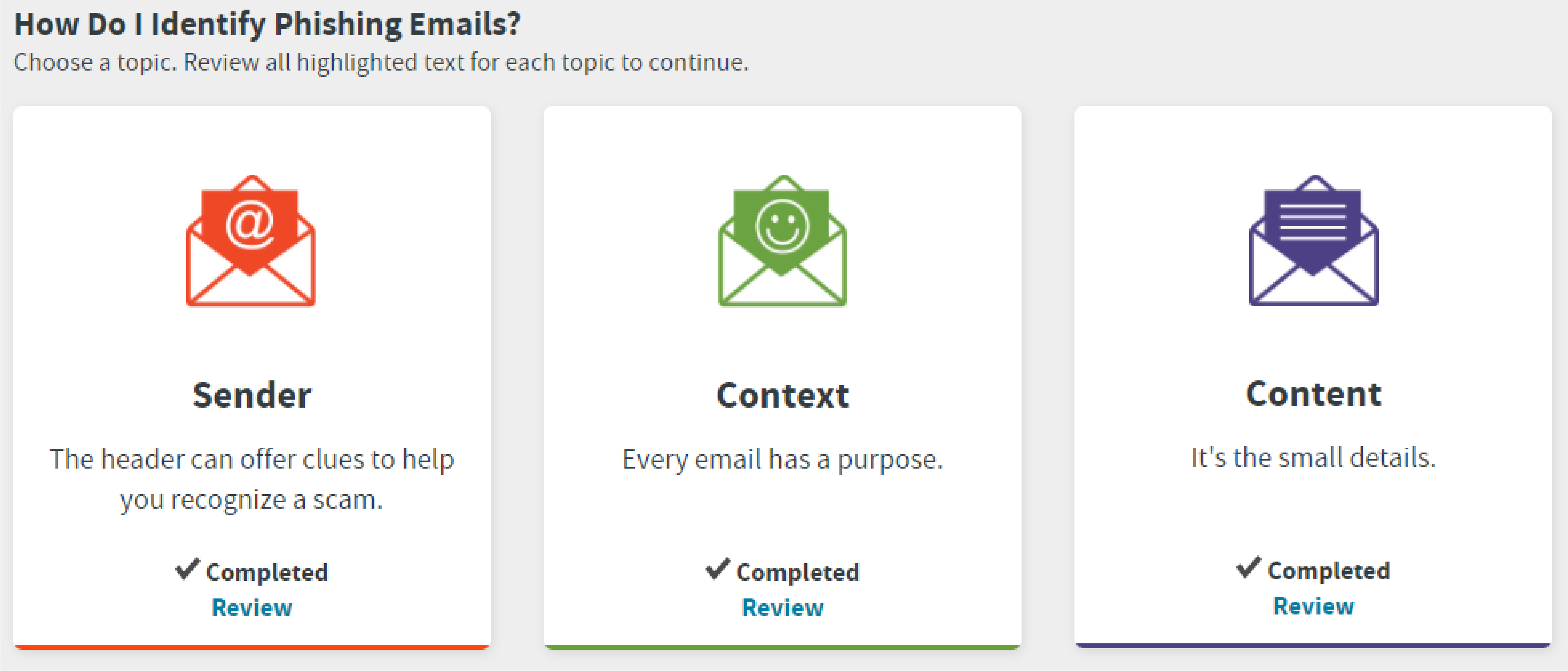
Click here if you believe that the web page has been blocked by mistake.

Detection method: databases

Message generated at: 13:05:15

Click me..

PHISING



How Do I Identify Phishing Emails?

Choose a topic. Review all highlighted text for each topic to continue.

Sender

The header can offer clues to help you recognize a scam.

✓ Completed

Review

Context

Every email has a purpose.

✓ Completed

Review

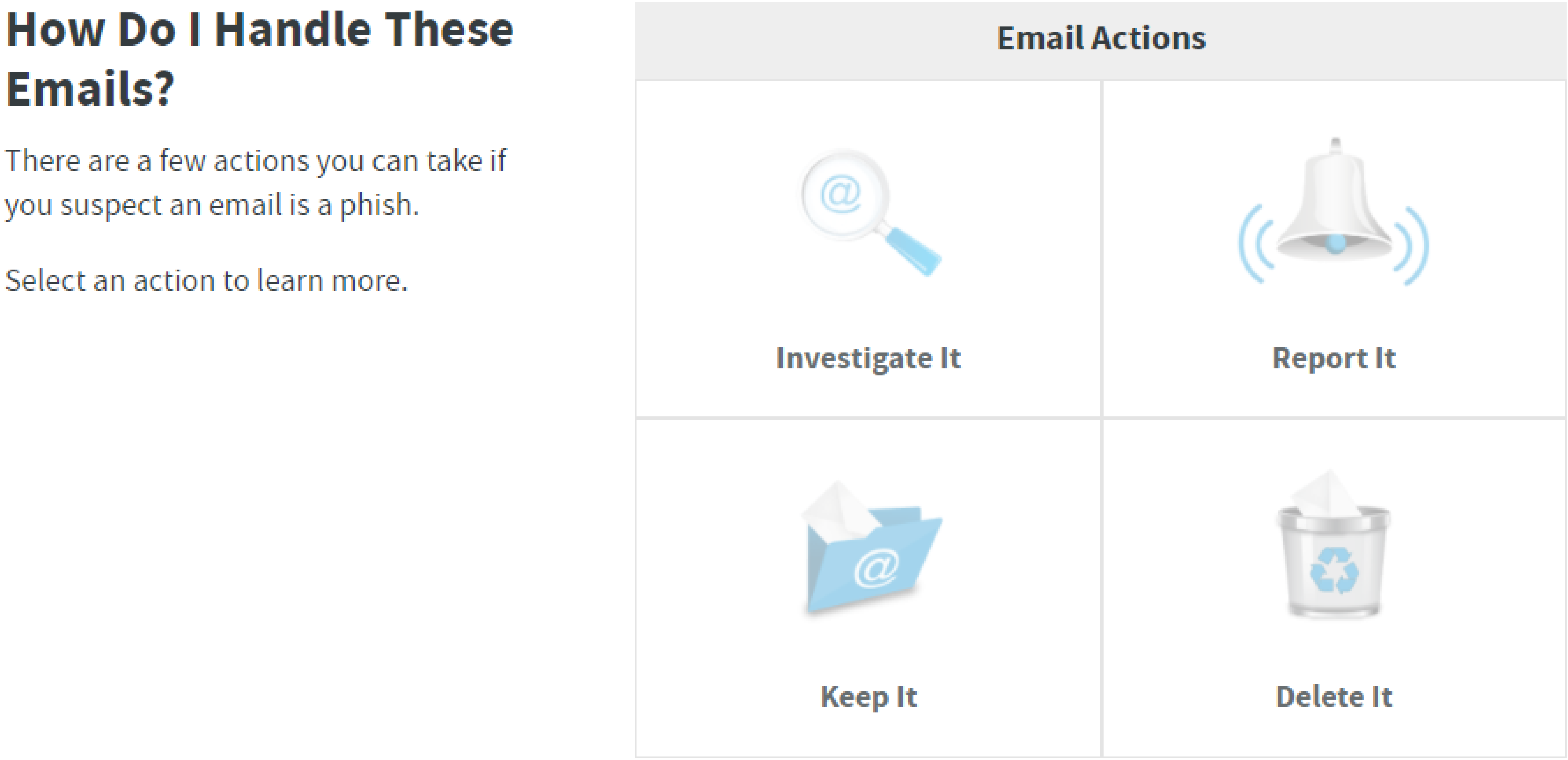
Content

It's the small details.

✓ Completed

Review

PHISING



How Do I Handle These Emails?

There are a few actions you can take if you suspect an email is a phish.

Select an action to learn more.

Email Actions

Investigate It	Report It
Keep It	Delete It

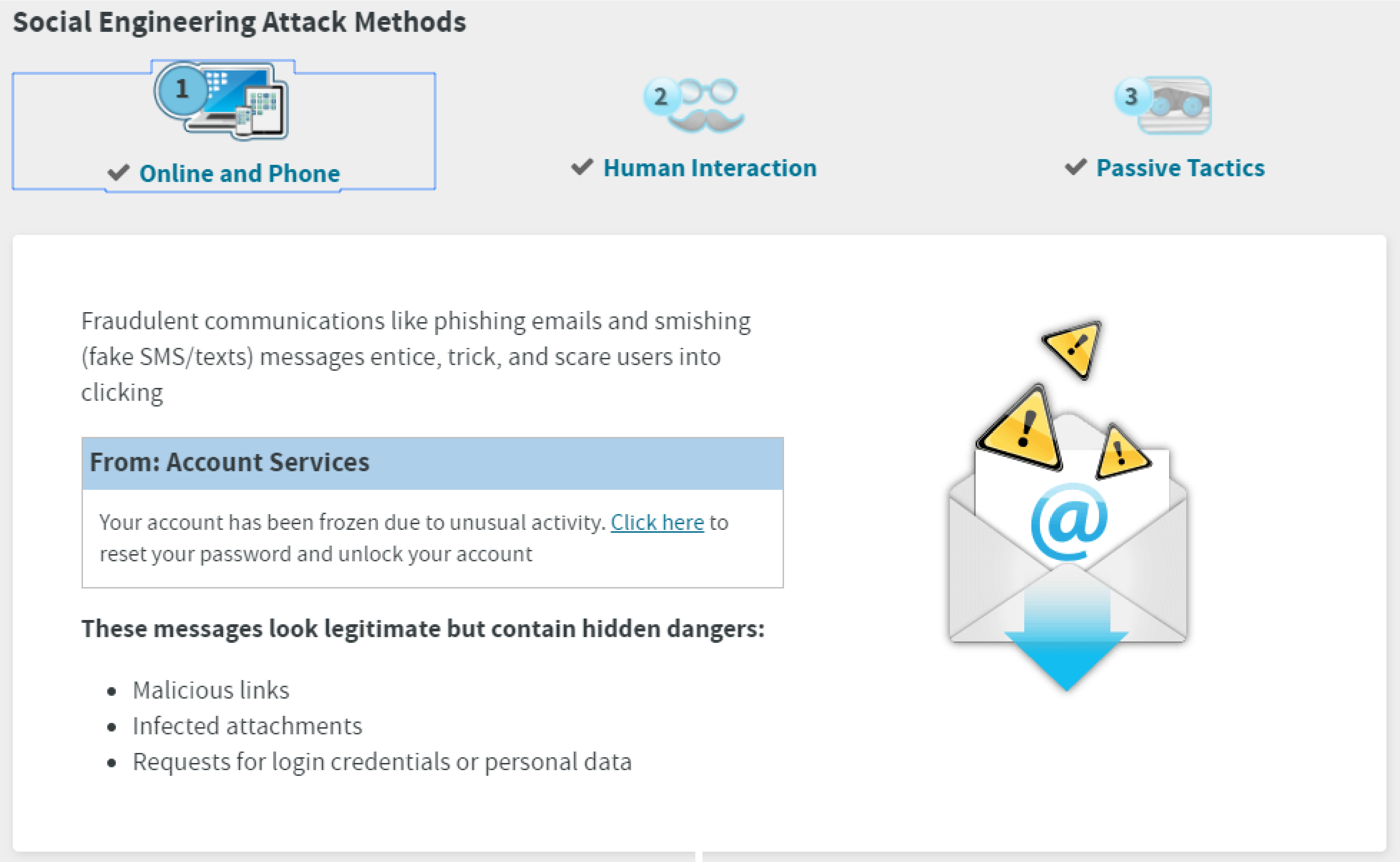
SOCIAL ENGINEERING

What Is Social Engineering?

Social engineering is a type of security attack where scammers trick people into giving them access to sensitive information

Social engineers have the same goal as hackers, but they focus on tricking people rather than breaking into networks

Sometimes the easiest way for scammers to gain the information they want is to ask for it



Social Engineering Attack Methods

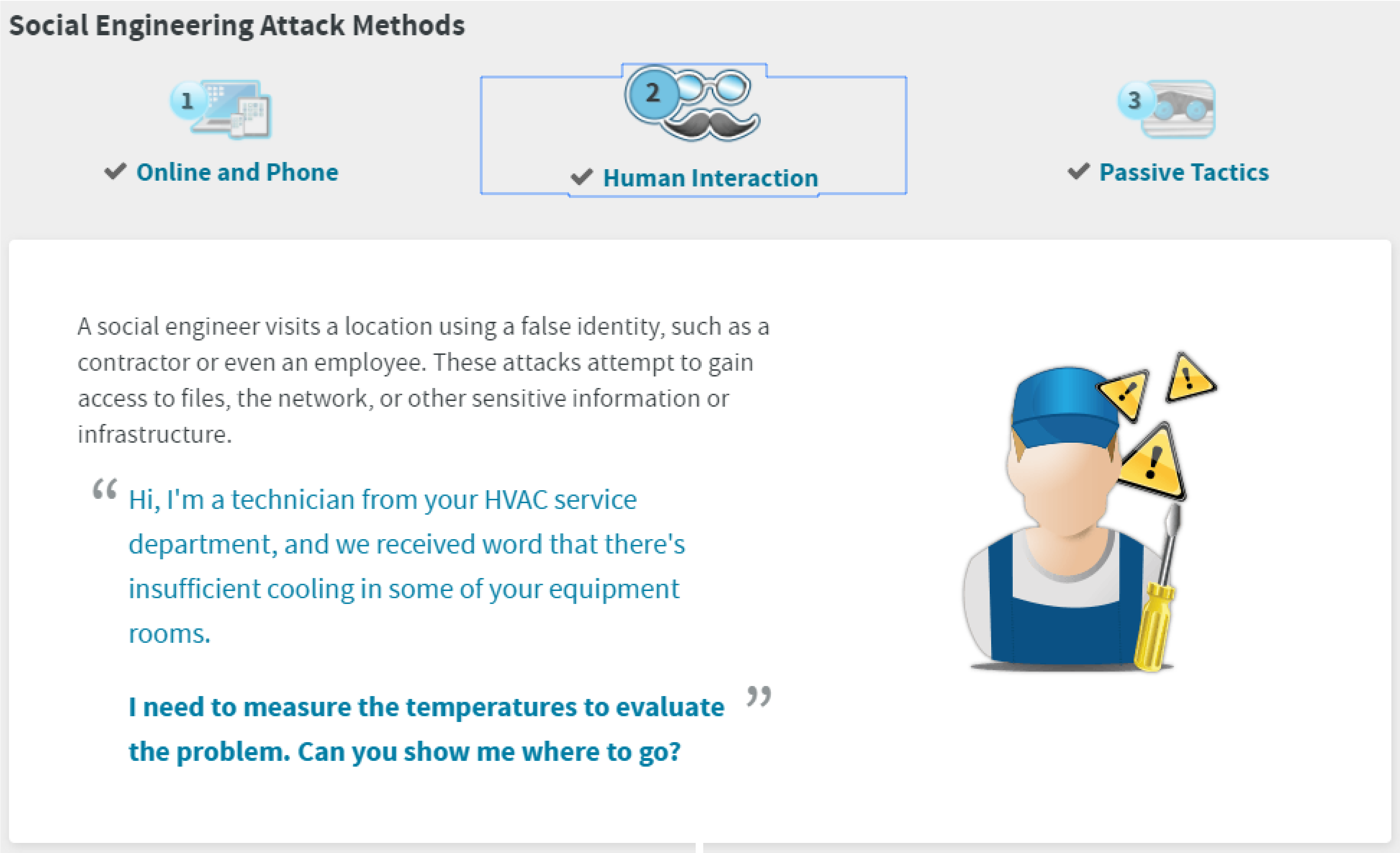
Fraudulent communications like phishing emails and smishing (fake SMS/texts) messages entice, trick, and scare users into clicking

From: Account Services

Your account has been frozen due to unusual activity. Click here to reset your password and unlock your account

These messages look legitimate but contain hidden dangers:

- Malicious links
- Infected attachments
- Requests for login credentials or personal data



Social Engineering Attack Methods

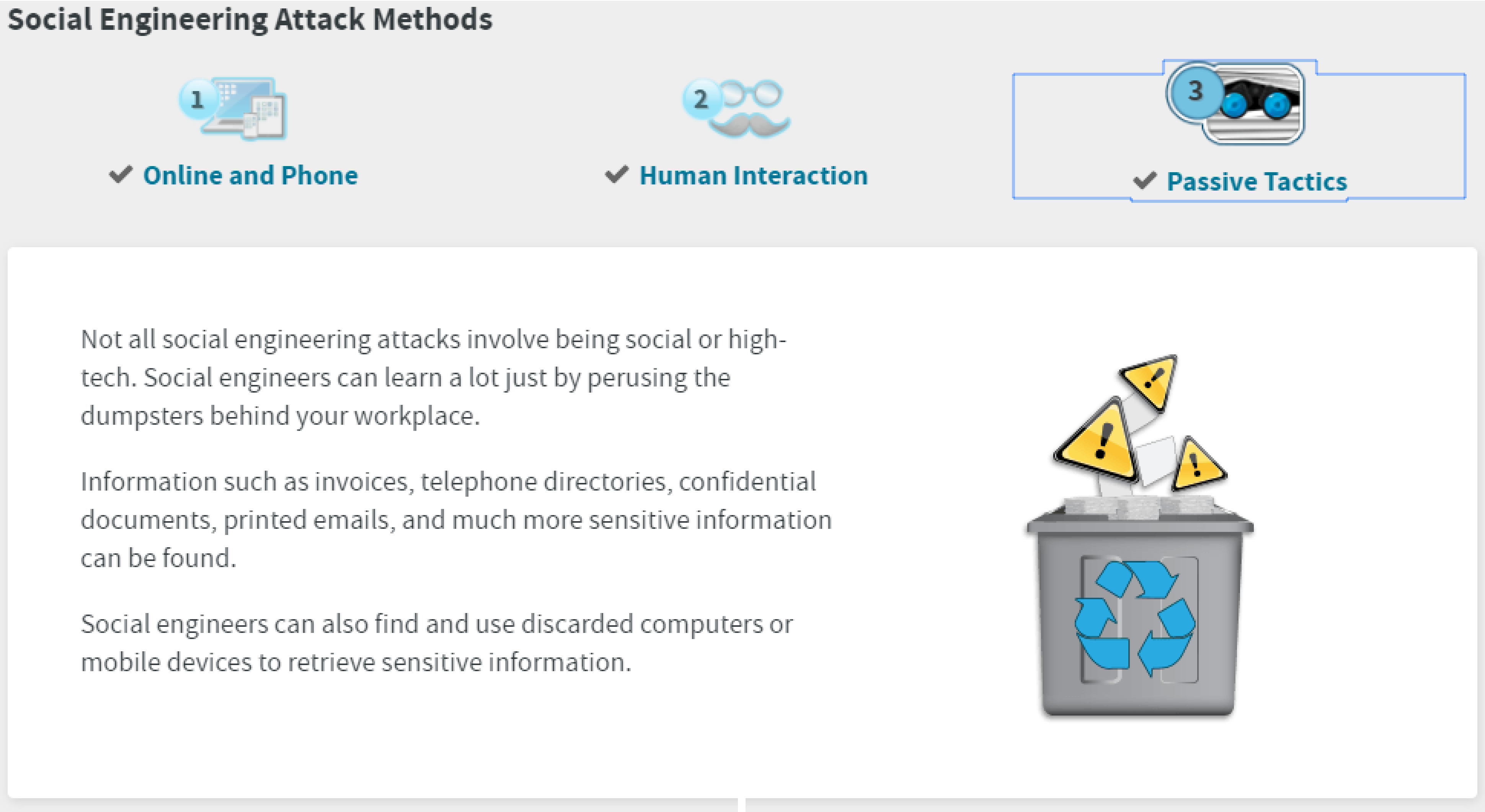
1 ✓ Online and Phone

2 ✓ Human Interaction

3 ✓ Passive Tactics

A social engineer visits a location using a false identity, such as a contractor or even an employee. These attacks attempt to gain access to files, the network, or other sensitive information or infrastructure.

> “Hi, I'm a technician from your HVAC service department, and we received word that there's insufficient cooling in some of your equipment rooms.
>
> **I need to measure the temperatures to evaluate the problem. Can you show me where to go?**”



Social Engineering Attack Methods

- ✓ Online and Phone
- ✓ Human Interaction
- ✓ Passive Tactics

Not all social engineering attacks involve being social or high-tech. Social engineers can learn a lot just by perusing the dumpsters behind your workplace.

Information such as invoices, telephone directories, confidential documents, printed emails, and much more sensitive information can be found.

Social engineers can also find and use discarded computers or mobile devices to retrieve sensitive information.

PASSWORDS

Why is password strength important?

! Choosing a strong password is the first line of defense in securing personal and business data.

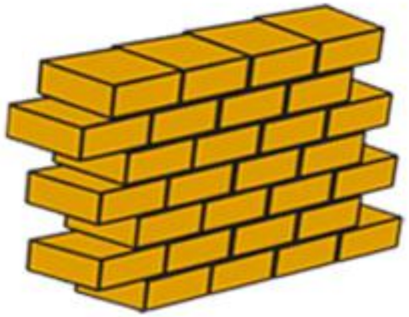
PASSWORDS

- Select a good one
  - At least 7 characters
  - Mixture of upper and lowercase characters
  - Mixture of alpha and numeric characters
  - Don’t use dictionary words
- Keep password safe
- Change them often
- Don’t share or reuse passwords
- Two Factor Authentication (2FA)

How do I create a strong password?

This lesson will teach you how to create two types of strong passwords:

1. Insertion
2. Phrase-based



ACCESS RIGHTS

ACCESS RIGHTS

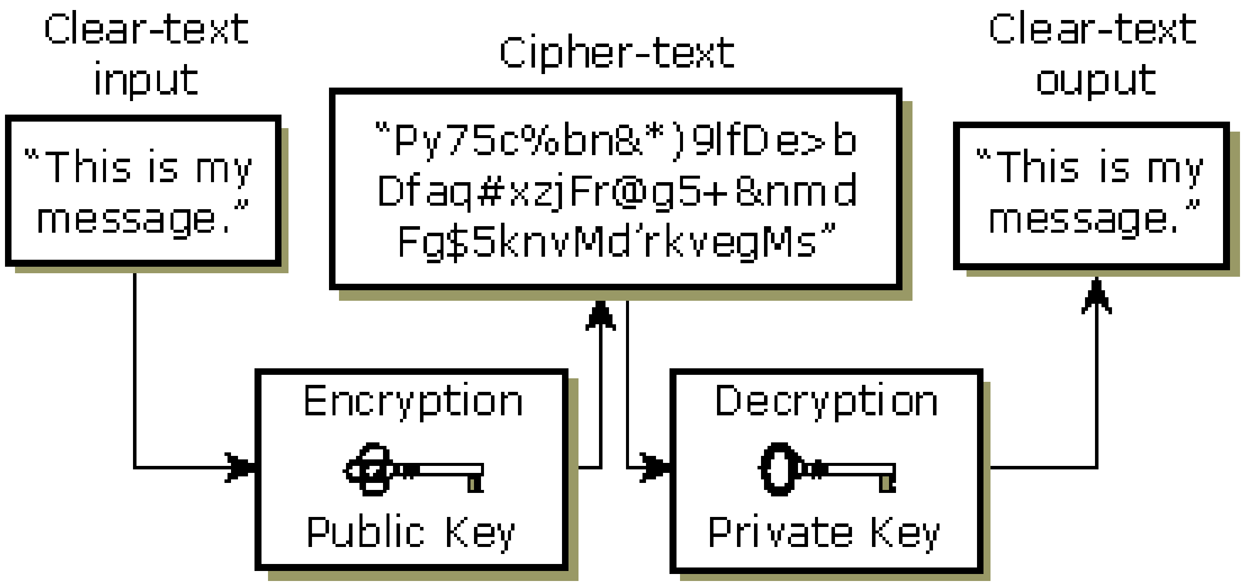
MALICIOUS & ACCIDENTAL

INSIDERS

- Excessive privileges
- Unmanaged passwords
- Accounts hijacked by attackers

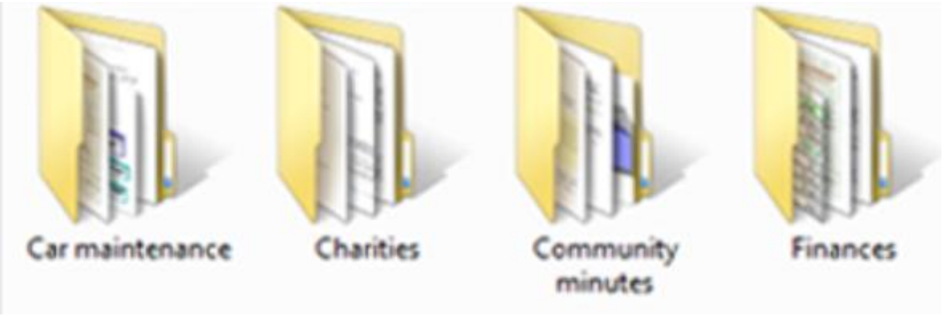
PROTECTING AGAINST RANSOMWARE

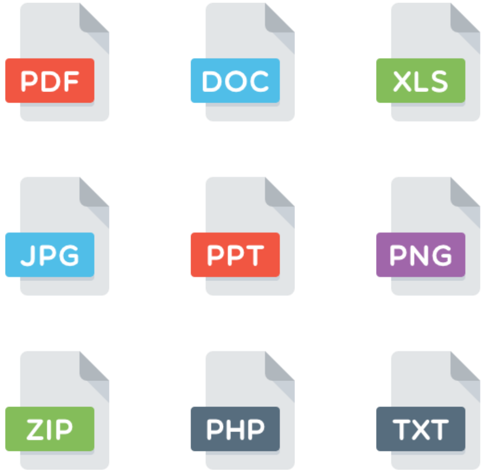
INTRODUCTION



IT WAS GOOD IN THE BEGINNING

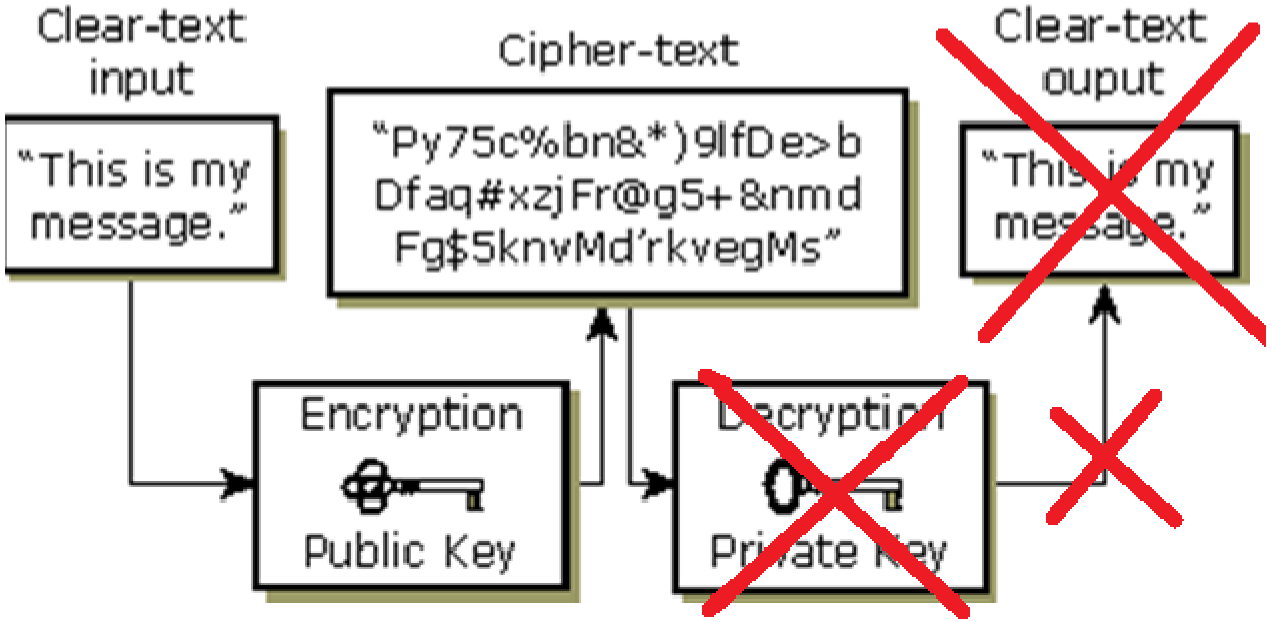
INTRODUCTION





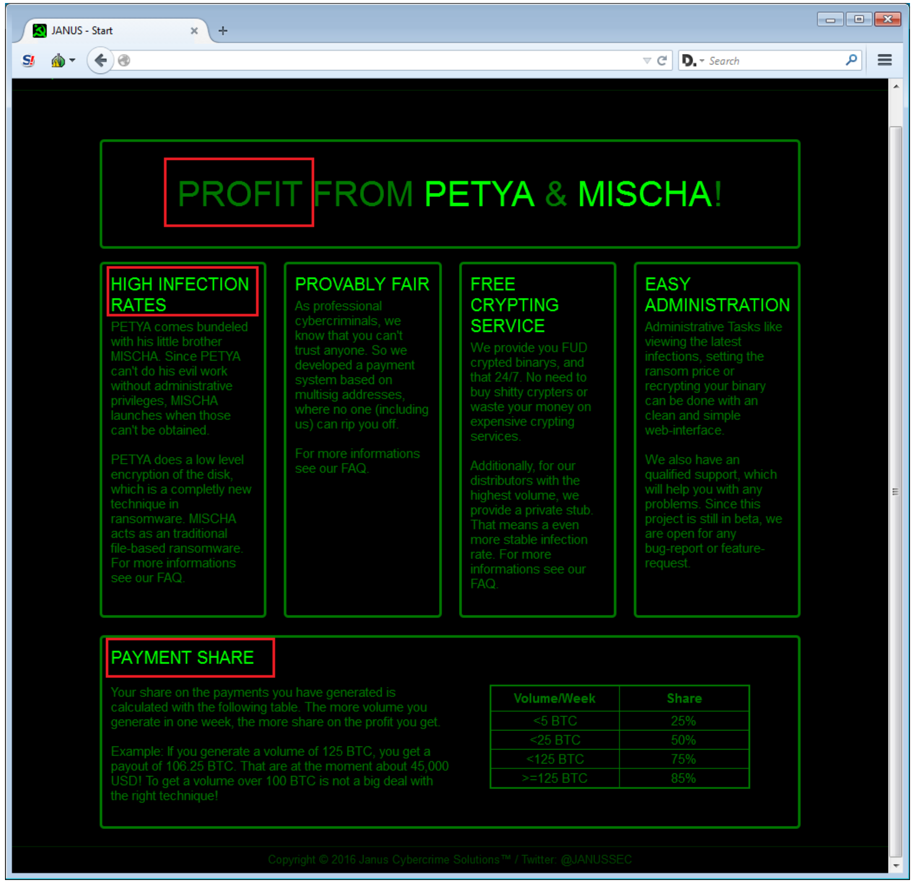
IT WAS DESIGNED AND BUILT TO PROTECT YOUR DATA CONFIDENTIALITY

WHAT IS RANSOMWARE



IT IS A MODIFIED ENCRYPTION TECHNOLOGY

MOTIVE AND AGENDA OF RANSOMWARE - EXAMPLES



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

FREE CRYPTING SERVICE

We provide you FUD crypted binarys, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.

Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.

EASY ADMINISTRATION

Administrative Tasks like viewing the latest infections, setting the ransom price or recrypting your binary can be done with an clean and simple web-interface.

We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

PAYMENT SHARE

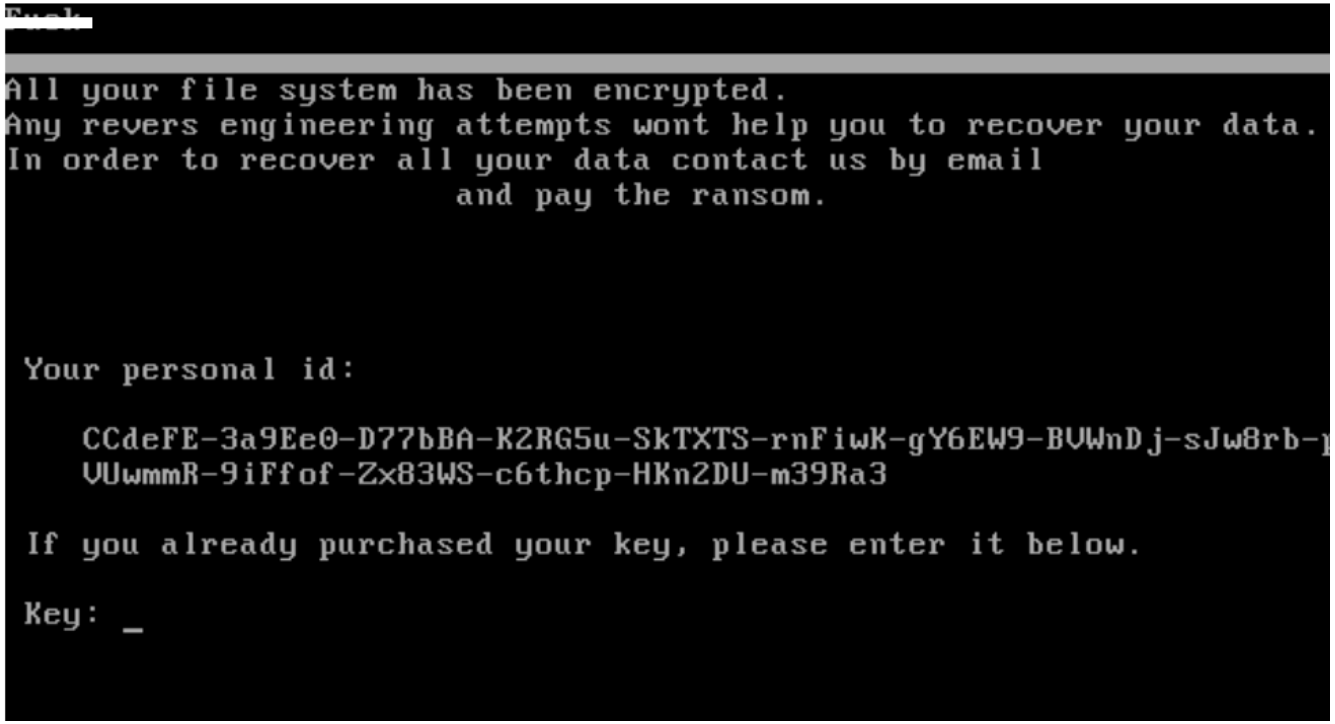
Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Copyright © 2016 Janus Cybercrime Solutions™ / Twitter: @JANUSSEC

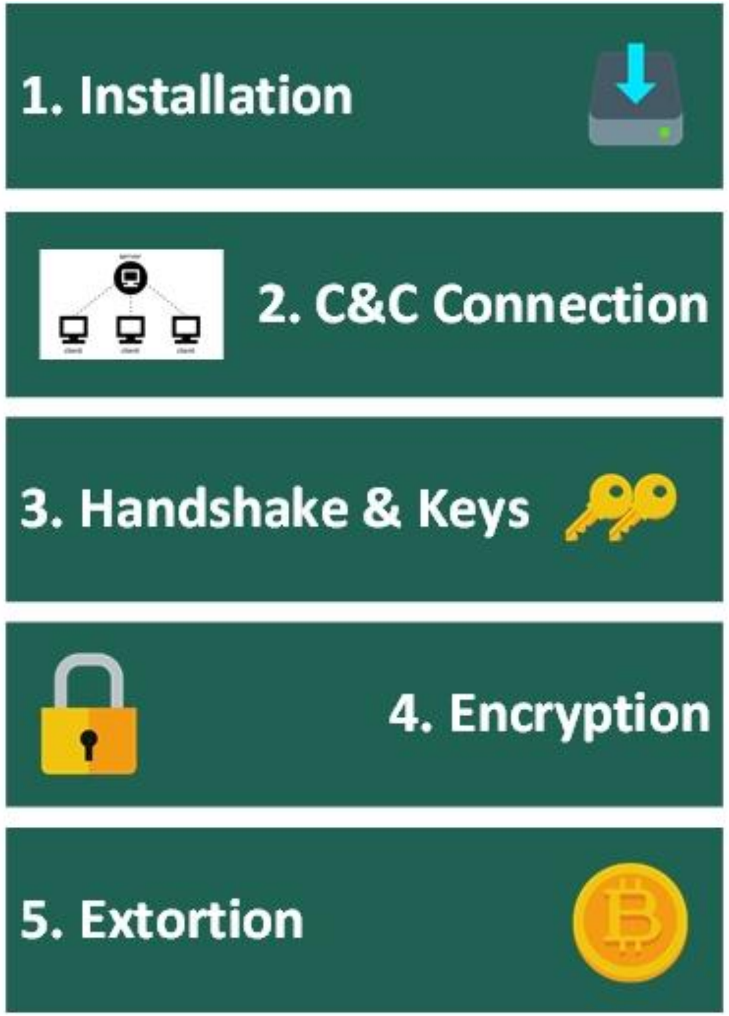
COMMERCIAL



```
[redacted]

All your file system has been encrypted.
Any revers engineering attempts wont help you to recover your data.
In order to recover all your data contact us by email
                 and pay the ransom.



 Your personal id:

    CCdeFE-3a9Ee0-D77bBA-K2RG5u-SkTXTS-rnFiwK-gY6EW9-BVWnDj-sJw8rb-
    VUwmmR-9iFfof-Zx83WS-c6thcp-HKn2DU-m39Ra3

 If you already purchased your key, please enter it below.

 Key: _
```

TARGETED ATTACK

GENERAL ANATOMY OF RANSOMWARE



1. Installation

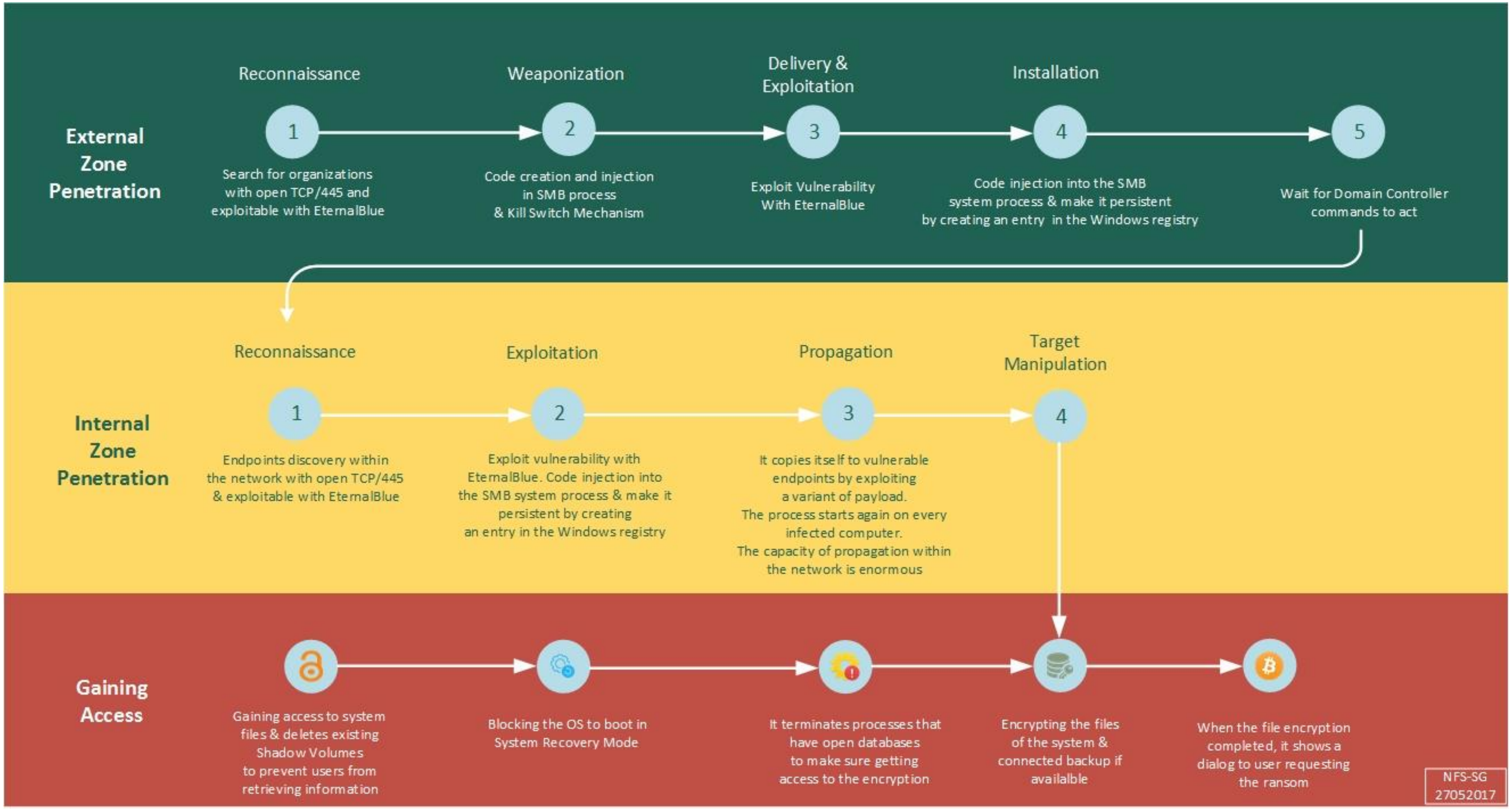
2. C&C Connection

3. Handshake & Keys

4. Encryption

5. Extortion

THE ANATOMY OF WANNACRY



External Zone Penetration

1. Reconnaissance: Search for organizations with open TCP/445 and exploitable with EternalBlue
2. Weaponization: Code creation and injection in SMB process & Kill Switch Mechanism
3. Delivery & Exploitation: Exploit Vulnerability With EternalBlue
4. Installation: Code injection into the SMB system process & make it persistent by creating an entry in the Windows registry
5. Wait for Domain Controller commands to act

Internal Zone Penetration

1. Reconnaissance: Endpoints discovery within the network with open TCP/445 & exploitable with EternalBlue
2. Exploitation: Exploit vulnerability with EternalBlue. Code injection into the SMB system process & make it persistent by creating an entry in the Windows registry
3. Propagation: It copies itself to vulnerable endpoints by exploiting a variant of payload. The process starts again on every infected computer. The capacity of propagation within the network is enormous
4. Target Manipulation

Gaining Access

Gaining access to system files & deletes existing Shadow Volumes to prevent users from retrieving information

Blocking the OS to boot in System Recovery Mode

It terminates processes that have open databases to make sure getting access to the encryption

Encrypting the files of the system & connected backup if availalble

When the file encryption completed, it shows a dialog to user requesting the ransom

NFS-SG 27052017

WANNACRY RANSOMWARE

- **First** worming Ransomware & **Largest** infection in history
- **WannaCrypt** incorporates leaked Equation exploit to self-spread
- **Drastically** decreased by Monday (15th May)
- **Kill Switches** save the day (for now)

WANNACRY RANSOMWARE

VARIANTS & KILL-SWITCHES

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com
- A no kill switch version hasn’t been detected in the wild yet

WANNACRY RANSOMWARE

THE FIRST 6 HOURS

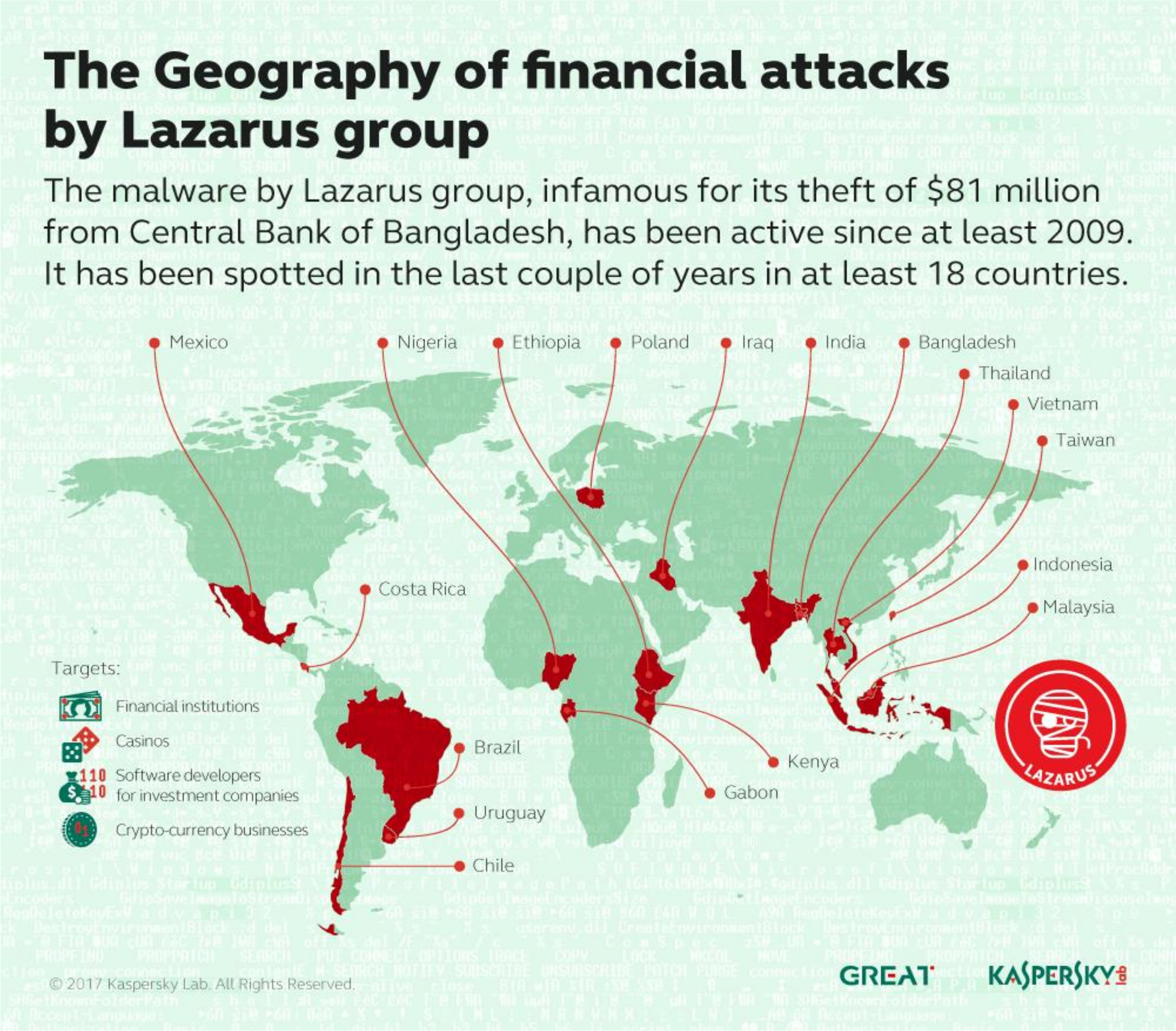
- **More than 7,000 machines** – during the 1st hour only
- **10,000** – number of machines stopped from infected further machines & having their data destroyed

WANNACRY RANSOMWARE

VICTIM STATISTIC

- **Kaspersky Security Network (KSN)** – 74 countries affected
- **MalwareTech + Comae Sinkhole** – 378,075 (prevented)
- Propagation is exponential – the more machines infected, the faster WannaCry multiplies

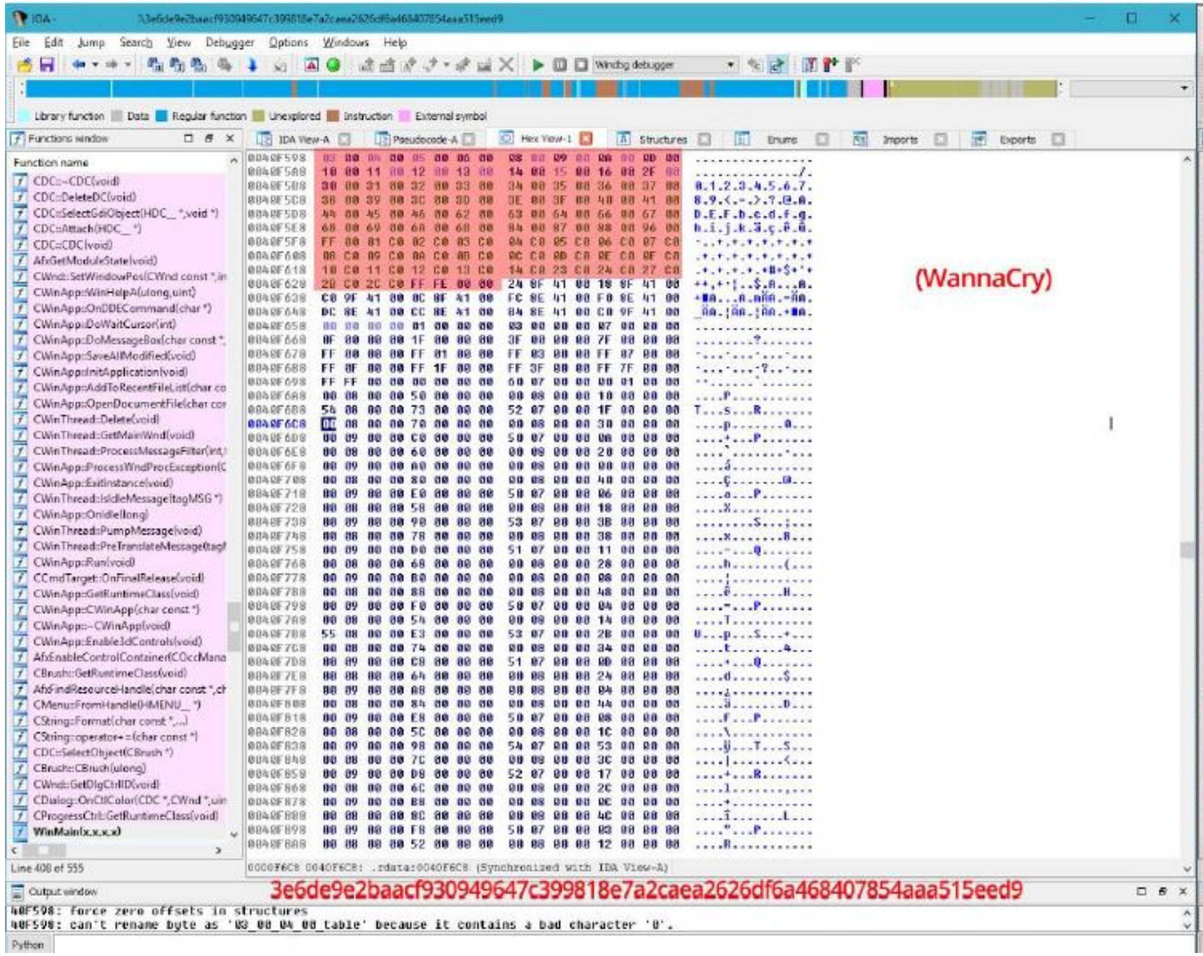
WANNACRY RANSOMWARE – LAZARUS GROUP



The Geography of financial attacks by Lazarus group

The malware by Lazarus group, infamous for its theft of $81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.

WANNACRY RANSOMWARE – IDENTICAL ARRAY USED



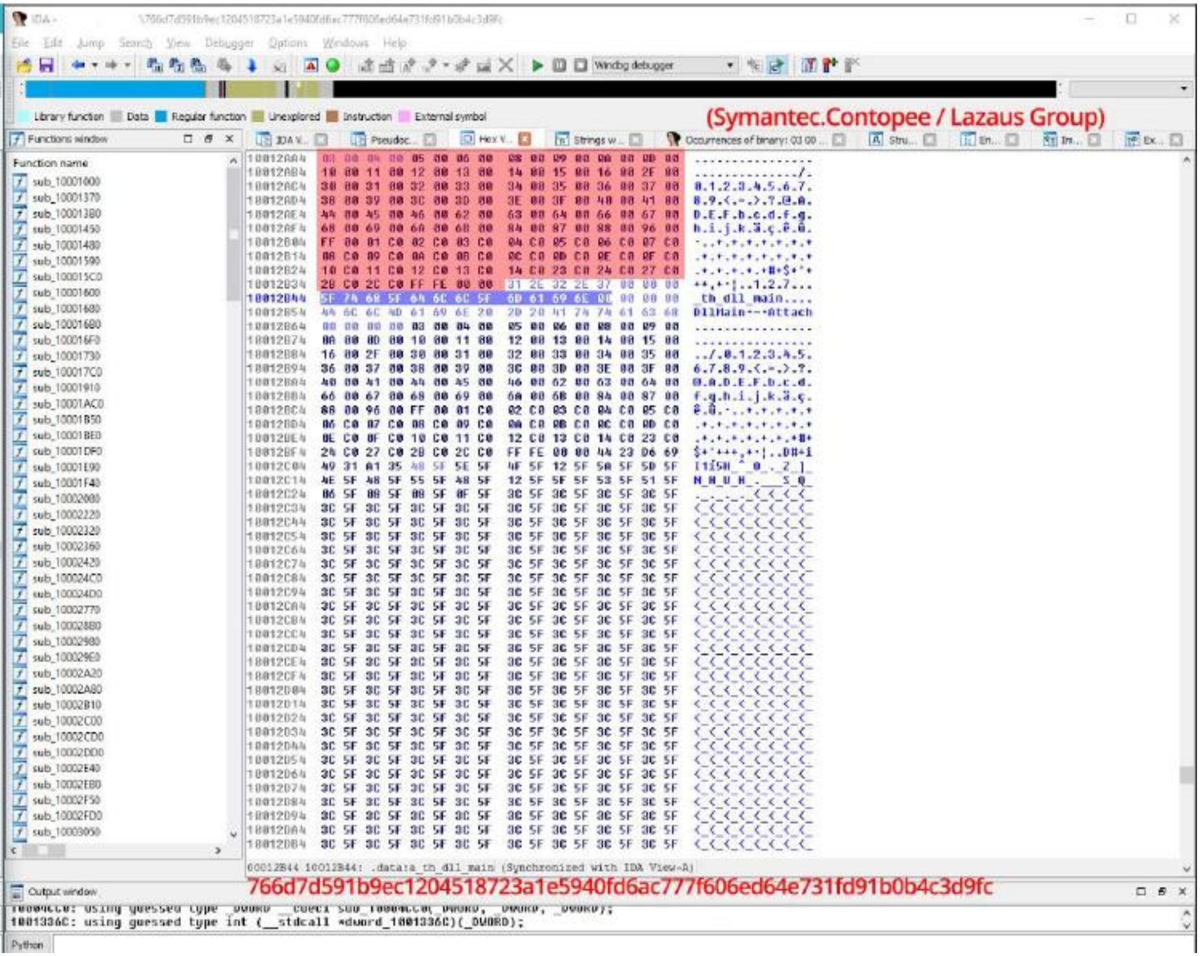
(WannaCry)

```
0040F598  03 00 04 00 05 00 06 00  08 00 09 00 0A 00 0D 00  ................
0040F5A8  10 00 11 00 12 00 13 00  14 00 15 00 16 00 2F 00  .............../.
0040F5B8  30 00 31 00 32 00 33 00  34 00 35 00 36 00 37 00  0.1.2.3.4.5.6.7.
0040F5C8  38 00 39 00 3C 00 3D 00  3E 00 3F 00 40 00 41 00  8.9.<.=.>.?.@.A.
0040F5D8  44 00 45 00 46 00 62 00  63 00 64 00 66 00 67 00  D.E.F.b.c.d.f.g.
0040F5E8  68 00 69 00 6A 00 6B 00  84 00 87 00 88 00 96 00  h.i.j.k.....
0040F5F8  FF 00 01 C0 02 C0 03 C0  04 C0 05 C0 06 C0 07 C0
0040F608  08 C0 09 C0 0A C0 0B C0  0C C0 0D C0 0E C0 0F C0
0040F618  10 C0 11 C0 12 C0 13 C0  14 C0 23 C0 24 C0 27 C0
0040F628  2B C0 2C C0 FF FE 00 00  24 8F 41 00 18 8F 41 00
```

```
0000F6C8 0040F6C8: .rdata:0040F6C8 (Synchronized with IDA View-A)
```

3e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9

```
40F598: force zero offsets in structures
40F598: can't rename byte as '03_00_04_00_table' because it contains a bad character '0'.
```



(Symantec.Contopee / Lazaus Group)

```
10012AA4  03 00 04 00 05 00 06 00  08 00 09 00 0A 00 0D 00  ................
10012AB4  10 00 11 00 12 00 13 00  14 00 15 00 16 00 2F 00  .............../.
10012AC4  30 00 31 00 32 00 33 00  34 00 35 00 36 00 37 00  0.1.2.3.4.5.6.7.
10012AD4  38 00 39 00 3C 00 3D 00  3E 00 3F 00 40 00 41 00  8.9.<.=.>.?.@.A.
10012AE4  44 00 45 00 46 00 62 00  63 00 64 00 66 00 67 00  D.E.F.b.c.d.f.g.
10012AF4  68 00 69 00 6A 00 6B 00  84 00 87 00 88 00 96 00  h.i.j.k.....
10012B04  FF 00 01 C0 02 C0 03 C0  04 C0 05 C0 06 C0 07 C0
10012B14  08 C0 09 C0 0A C0 0B C0  0C C0 0D C0 0E C0 0F C0
10012B24  10 C0 11 C0 12 C0 13 C0  14 C0 23 C0 24 C0 27 C0
10012B34  2B C0 2C C0 FF FE 00 00  31 2E 32 2E 37 00 00 00  ++,+...1.2.7...
10012B44  5F 74 68 5F 64 6C 6C 5F  6D 61 69 6E 00 00 00 00  _th_dll_main....
10012B54  44 6C 6C 4D 61 69 6E 20  2D 2D 41 74 74 61 63 68  DllMain--Attach
```

```
00012B44 10012B44: .data:a_th_dll_main (Synchronized with IDA View-A)
```

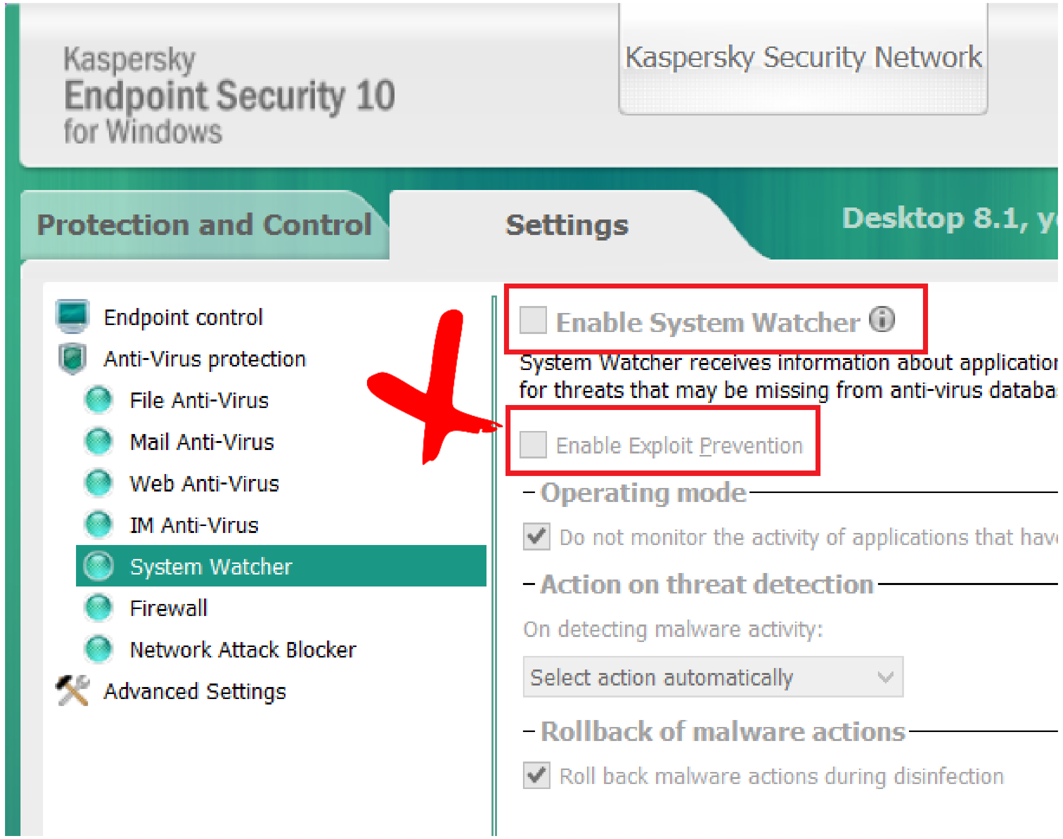
766d7d591b9ec1204518723a1e5940fd6ac777f606ed64e731fd91b0b4c3d9fc

```
1001336C: using guessed type int (__stdcall *dword_1001336C)(_DWORD);
```

WANNACRY RANSOMWARE – FAQ

- **Does the WannaCRY need admin privileges** – no, the infection is done via kernel exploitation which ensure total control of the machine to the attacker.
- **Can encrypted files be recovered** – No viable solution to recover the encrypted files had been found yet. Private key is destroyed in memory very early.
- **Did Microsoft released patches for those vulnerabilities** – Yes, MS17-010 in March (Vista+), KB4012598 on Friday 14 (< Vista)

BIG MISTAKES – KASPERKY LAB USERS



Kaspersky
Endpoint Security 10
for Windows

Kaspersky Security Network

Protection and Control | Settings | Desktop 8.1, y

- Endpoint control
- Anti-Virus protection
  - File Anti-Virus
  - Mail Anti-Virus
  - Web Anti-Virus
  - IM Anti-Virus
  - System Watcher
  - Firewall
  - Network Attack Blocker
- Advanced Settings

□ Enable System Watcher

System Watcher receives information about applicatio
for threats that may be missing from anti-virus databa

□ Enable Exploit Prevention

– Operating mode

☑ Do not monitor the activity of applications that hav

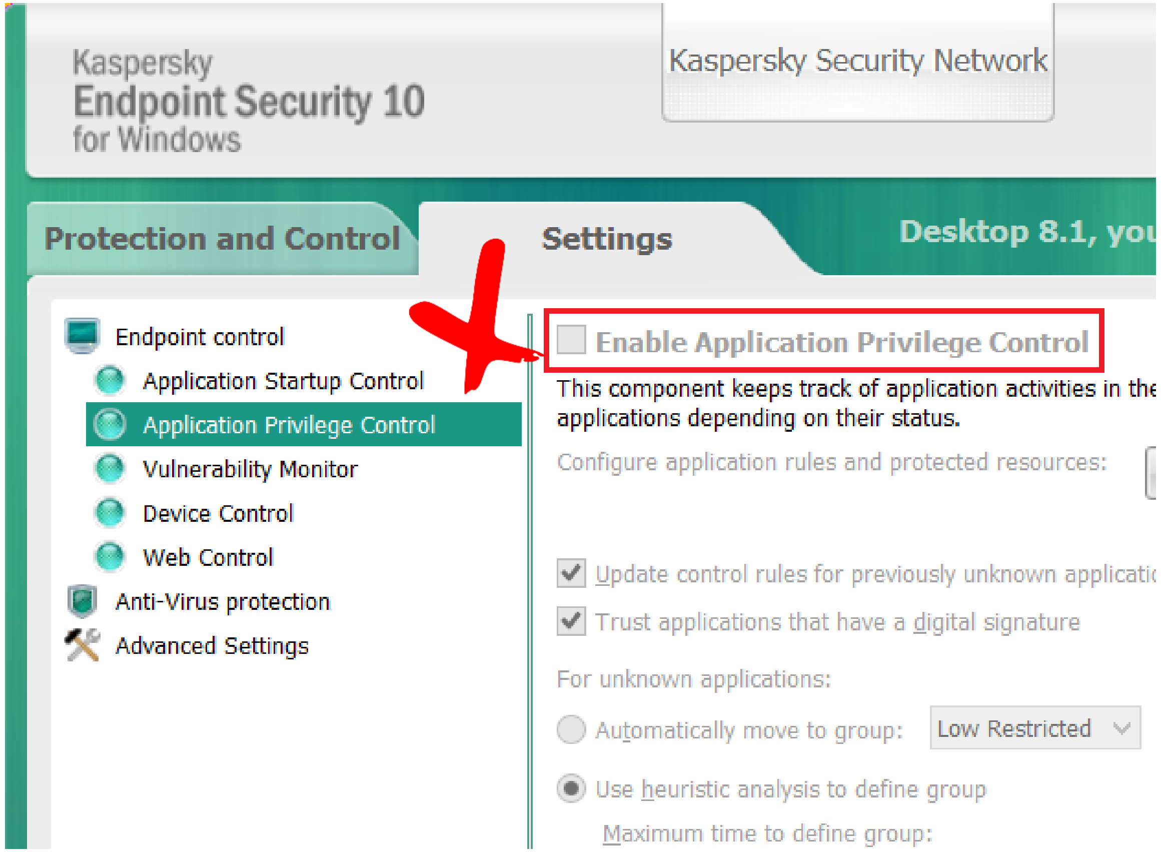
– Action on threat detection

On detecting malware activity:

Select action automatically

– Rollback of malware actions

☑ Roll back malware actions during disinfection



Kaspersky
Endpoint Security 10
for Windows

Kaspersky Security Network

Protection and Control | Settings | Desktop 8.1, you

- Endpoint control
  - Application Startup Control
  - Application Privilege Control
  - Vulnerability Monitor
  - Device Control
  - Web Control
- Anti-Virus protection
- Advanced Settings

□ Enable Application Privilege Control

This component keeps track of application activities in the
applications depending on their status.

Configure application rules and protected resources:

☑ Update control rules for previously unknown applicati

☑ Trust applications that have a digital signature

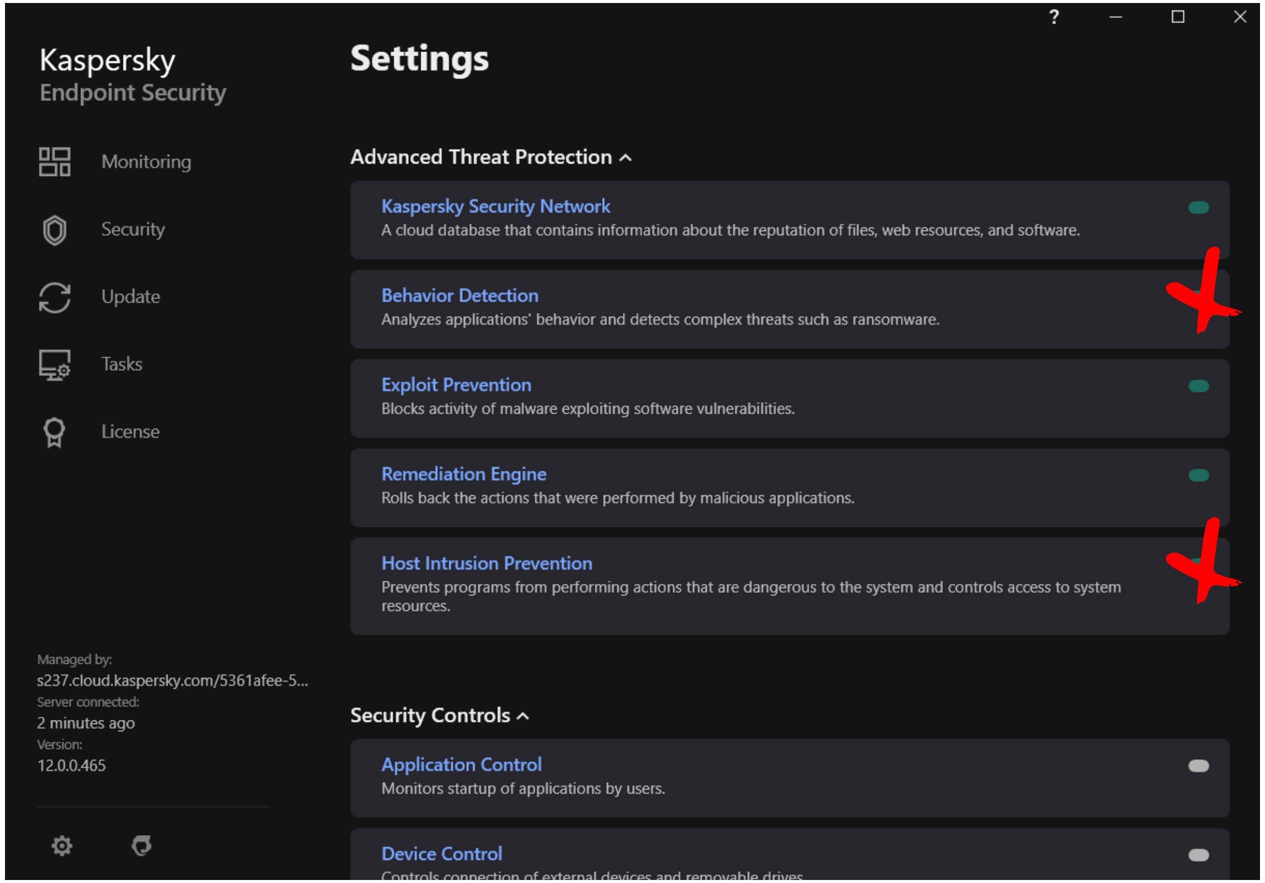
For unknown applications:

○ Automatically move to group: Low Restricted

● Use heuristic analysis to define group

Maximum time to define group:

BIG MISTAKES – KASPERKY LAB USERS



Kaspersky
Endpoint Security

Settings

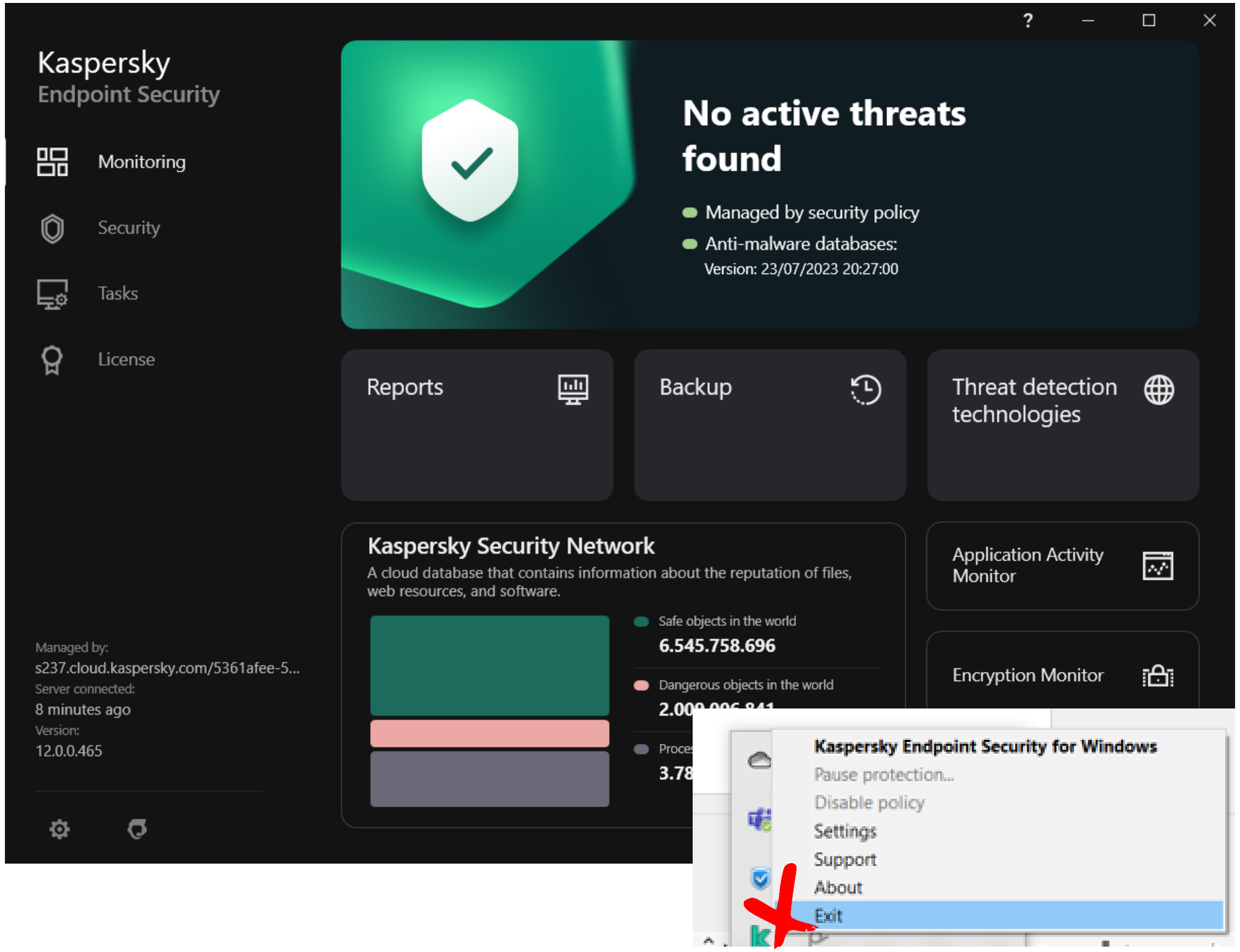
Advanced Threat Protection ^

- **Kaspersky Security Network** — A cloud database that contains information about the reputation of files, web resources, and software.
- **Behavior Detection** — Analyzes applications' behavior and detects complex threats such as ransomware.
- **Exploit Prevention** — Blocks activity of malware exploiting software vulnerabilities.
- **Remediation Engine** — Rolls back the actions that were performed by malicious applications.
- **Host Intrusion Prevention** — Prevents programs from performing actions that are dangerous to the system and controls access to system resources.

Security Controls ^

- **Application Control** — Monitors startup of applications by users.
- **Device Control** — Controls connection of external devices and removable drives

Managed by:
s237.cloud.kaspersky.com/5361afee-5...
Server connected:
2 minutes ago
Version:
12.0.0.465



Kaspersky
Endpoint Security

No active threats found

- Managed by security policy
- Anti-malware databases:
  Version: 23/07/2023 20:27:00

Kaspersky Security Network
A cloud database that contains information about the reputation of files, web resources, and software.

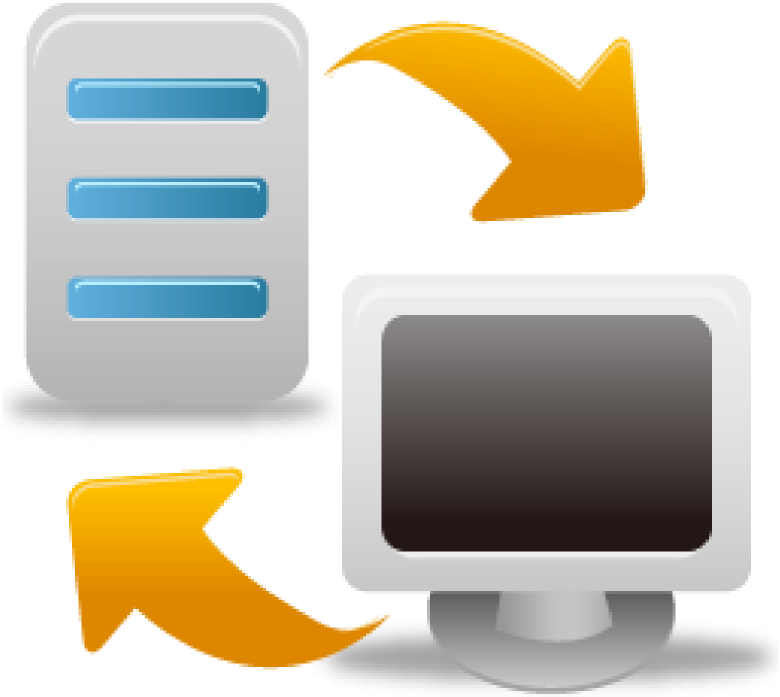
- Safe objects in the world: 6.545.758.696
- Dangerous objects in the world: 2.000.006.841
- Proce... 3.78...

Managed by:
s237.cloud.kaspersky.com/5361afee-5...
Server connected:
8 minutes ago
Version:
12.0.0.465

RANSOMWARE MITIGATION – TRADITIONAL WAY

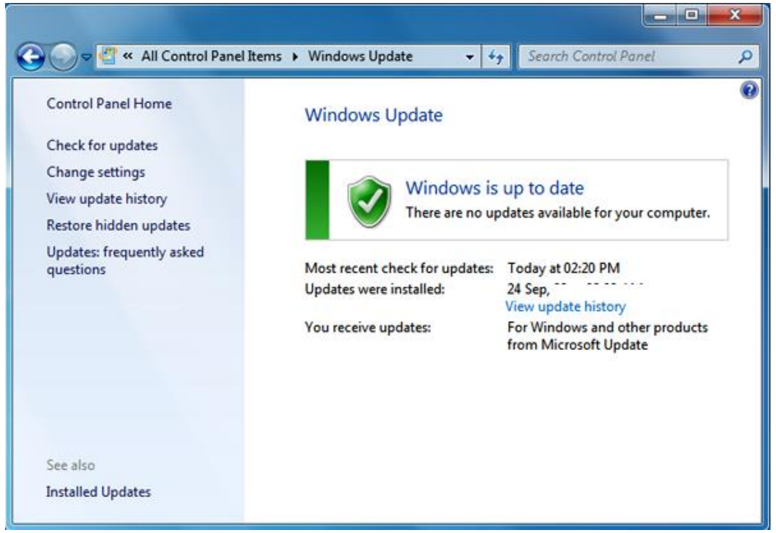
EDUCATE YOUR USERS

RANSOMWARE MITIGATION – TRADITIONAL WAY



DO REGULAR OFFLINE BACKUP AND TEST IT

RANSOMWARE MITIGATION – SOFTWARE UPDATES



Windows Update

Windows is up to date

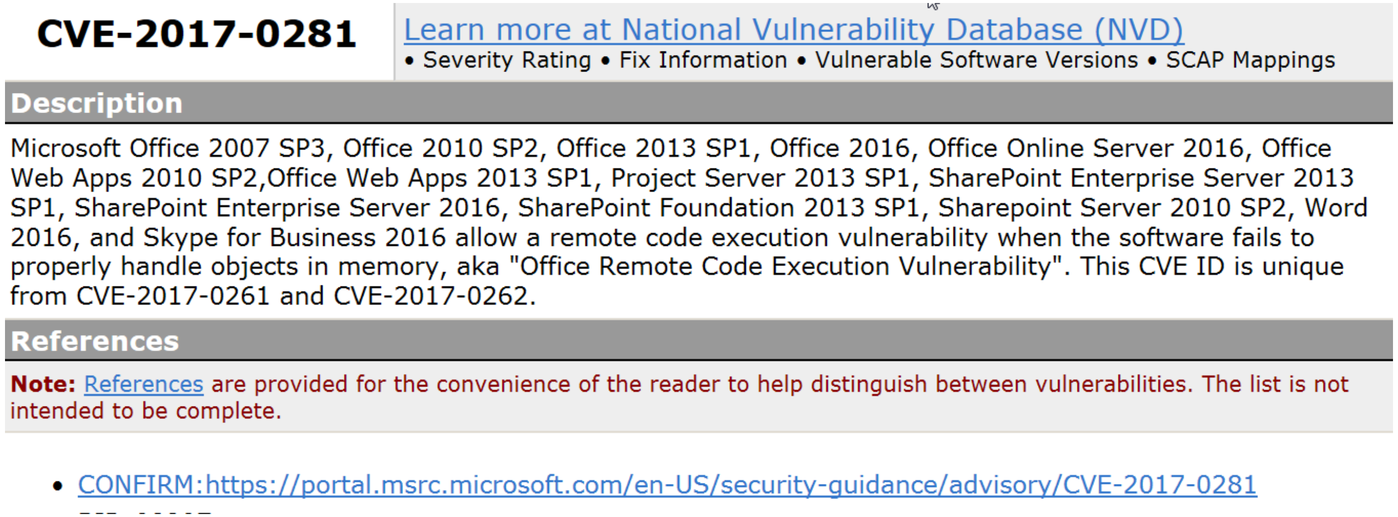
There are no updates available for your computer.

Most recent check for updates: Today at 02:20 PM

Updates were installed: 24 Sep,

View update history

You receive updates: For Windows and other products from Microsoft Update



CVE-2017-0281

Learn more at National Vulnerability Database (NVD)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2016, Office Online Server 2016, Office Web Apps 2010 SP2,Office Web Apps 2013 SP1, Project Server 2013 SP1, SharePoint Enterprise Server 2013 SP1, SharePoint Enterprise Server 2016, SharePoint Foundation 2013 SP1, Sharepoint Server 2010 SP2, Word 2016, and Skype for Business 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0261 and CVE-2017-0262.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0281

UPDATE ALL OPERATING SYSTEM(S) AND APPLICATION(S) ON ALL NODES

RANSOMWARE MITIGATION – POLICIES ENFORCEMENT

1. **Manage the use** of the Internet – for example according to the job role
2. **Control access** to corporate data – again, according to the job or department
3. **Manage the launch of the programs** – using Application Control technologies that help you to block or permit programs
4. **Segment your network**

MAKE SURE THAT PROPER POLICIES ARE ENFORCED

WANNACRY MITIGATION – PATCH INSTALLATION

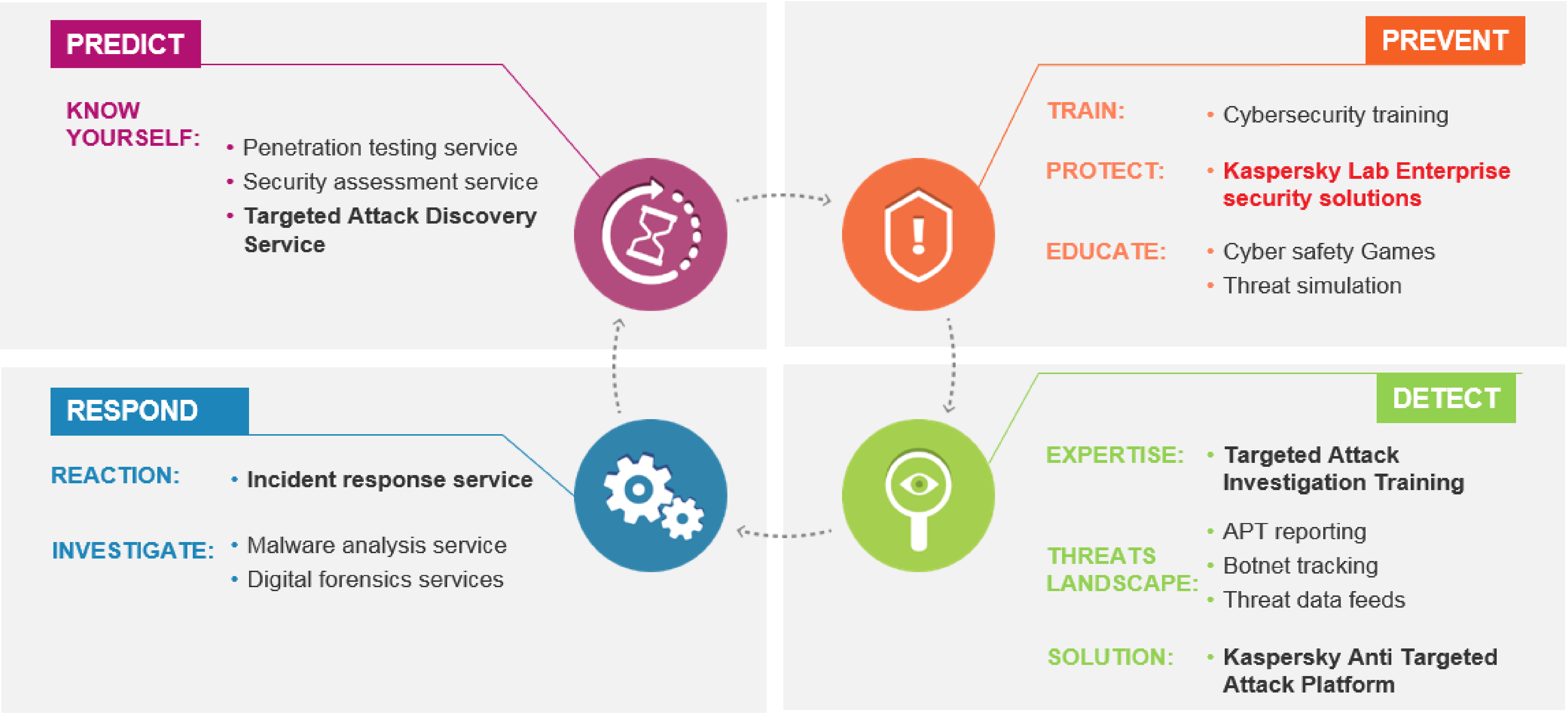
1. Install **Patch**
2. Make sure that **MS-17-010** is installed
3. **KB4012598** - Emergency patch released by Microsoft for XP & 2003
4. Disable **SMBv1**

IF POSSIBLE, AVOID USING OPERATING SYSTEM WHICH IS END OF LIFE

WANNACRY MITIGATION – NETWORK AND ENDPOINT

1. Network Level: block incoming traffic to **TCP/445**
2. Deploy **“Strong Heuristic”** Anti-Malware Solution
3. Free Antiransom Tool is available for business **https://go.kaspersky.com/Anti-ransomware-tool.html**
4. Kaspersky Lab users: make sure System Watcher is not disabled(**ON** by default)

KASPERSKY LAB ADAPTIVE SECURITY STRATEGY



PREDICT

KNOW YOURSELF:
- Penetration testing service
- Security assessment service
- **Targeted Attack Discovery Service**

PREVENT

TRAIN:
- Cybersecurity training

PROTECT:
- **Kaspersky Lab Enterprise security solutions**

EDUCATE:
- Cyber safety Games
- Threat simulation

DETECT

EXPERTISE:
- **Targeted Attack Investigation Training**

THREATS LANDSCAPE:
- APT reporting
- Botnet tracking
- Threat data feeds

SOLUTION:
- **Kaspersky Anti Targeted Attack Platform**

RESPOND

REACTION:
- **Incident response service**

INVESTIGATE:
- Malware analysis service
- Digital forensics services

Now

Aaah! Something went wrong
Reboot.
It seems we are safe

User

IT Support/Admins

IT Security

Should be

Aaah! Something went wrong
Let's check...
We are really safe now!

User

IT Support/Admins

IT Security

Q&A

LET'S TALK?

Ary Pryanto

Klabs Certified Consultant

www.vstecsindo.net