INFOSEC
INFORMATION SECURITY SOLUTIONS

Areg Shmavonyan
<<InfoSec>> LLC

04.10.2024

TABLE OF CONTENTS

INFOSEC
INFORMATION SECURITY SOLUTIONS

INTRODUCTION

Ransomware is a type of **crypto virus** designed to block access or encrypt data, with hackers holding the decryption key until a ransom is paid. Unlike trojans or other malware, ransomware focuses solely on encrypting files and has become a growing threat worldwide.

INFOSEC
INFORMATION SECURITY SOLUTIONS

Ransomware attacks

WannaCry

- Affected over **200,000 computers** across **150 countries** in just a *few days*, disrupting services in critical sectors like healthcare, finance, and telecommunications.
- The attack leveraged a vulnerability in **Microsoft Windows**, specifically the Server Message Block (SMB) protocol, known as **EternalBlue**. This exploit was reportedly developed by the **U.S. National Security Agency (NSA)** and later leaked by a hacker group called the Shadow Brokers.
- In April 2017, a hacker group known as the **Shadow Brokers** leaked EternalBlue and several other NSA exploits online. This leak allowed cybercriminals, including the creators of WannaCry, to access and use the exploit for malicious purposes.

INFOSEC
INFORMATION SECURITY SOLUTIONS

Ransomware attacks

WannaCry

- **Rapid Spread:** Once a computer was infected, WannaCry would **self-propagate** through the network, spreading *without any user intervention*.
- **Ransom Demand:** Victims were demanded to pay a ransom in **Bitcoin**, with the standard amount being $300. If payment wasn't made within 3 days, the ransom would double.

- **Kill Switch**: A cybersecurity researcher named Marcus Hutchins discovered a "kill switch" in the malware's code, which involved activating a dormant domain. By registering the domain, he was able to halt the spread of WannaCry.

INFOSEC
INFORMATION SECURITY SOLUTIONS

Estimates of Financial Impact

Damages Wanna Cry reached:

$4 000 000 000

Potential future losses:

$7 000 000 000 000

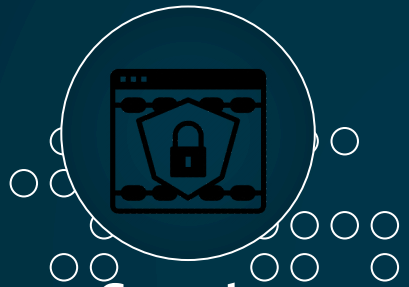
particularly due to the attack's disruption of essential services.

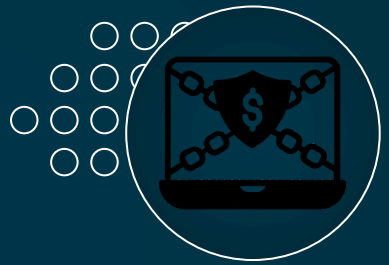
01 Types of Ransomware

(Crypto, Locker)

INFOSEC
INFORMATION SECURITY SOLUTIONS

Types of Ransomware





Crypto Ransomware

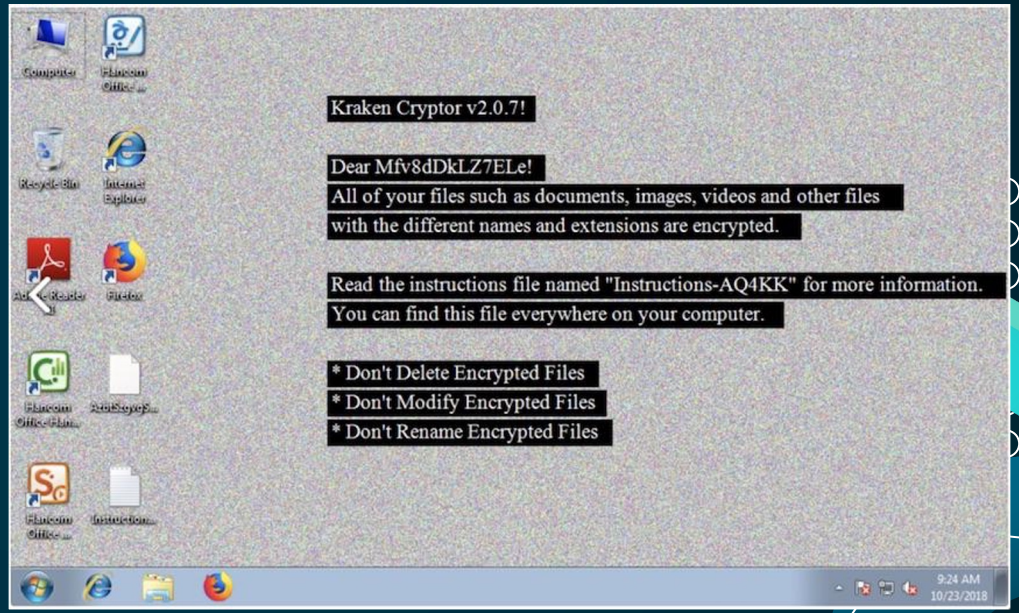
Encrypts files, making them inaccessible until a ransom is paid. Targets sensitive data, often rendering systems unusable.

Locker Ransomware

Locks the user out of their device entirely, preventing access to essential functions. Unlike crypto ransomware, files are not encrypted, but the device is unusable.

INFOSEC
INFORMATION SECURITY SOLUTIONS

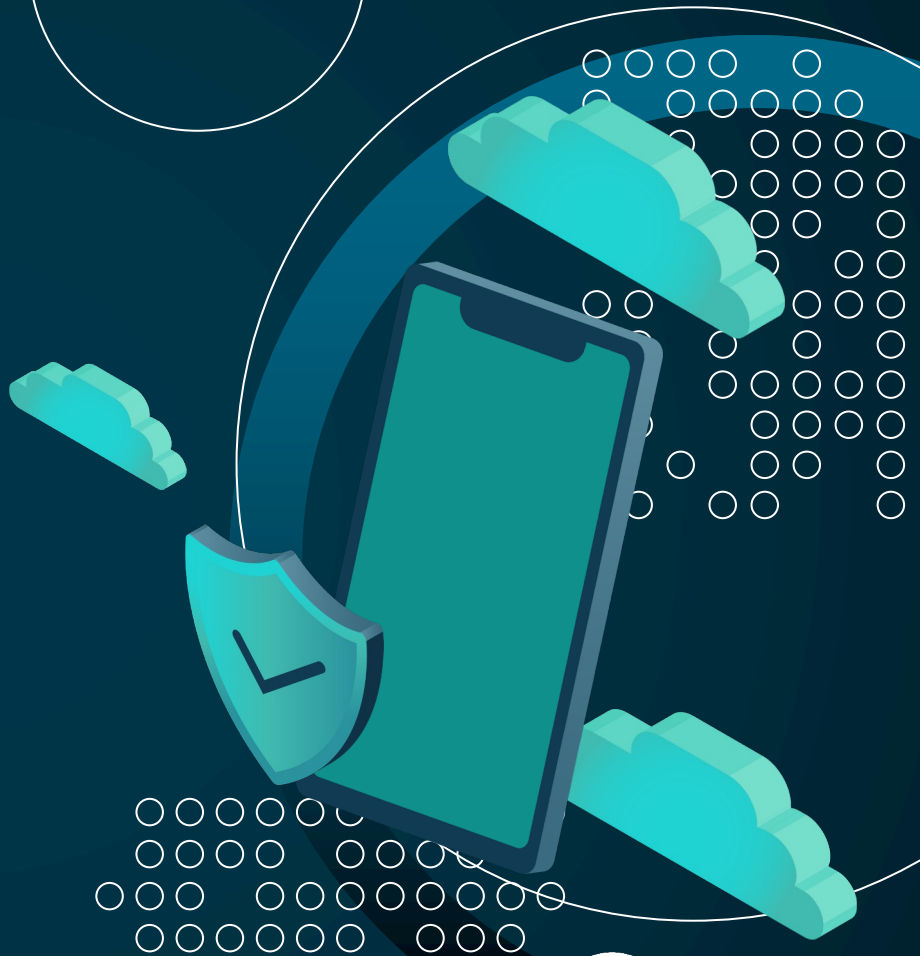

NoCry Decryptor
Oooooops All Your Files Are Encrypted ,NoCry
Can I Recover My Files ?
Yes, You Can Recover All Your Files Easily And Quickly
But How ?
Send The Required Amount And
I Will Send The Key To You For Decryption
See You Soon (0_0)
Your files will be lost on :
71 : 58
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
Send $100 worth of bitcoin to this address:
1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK
Copy
Show Encrypted Files
Decrypt


Kraken Cryptor v2.0.7!
Dear Mfv8dDkLZ7ELe!
All of your files such as documents, images, videos and other files
with the different names and extensions are encrypted.
Read the instructions file named "Instructions-AQ4KK" for more information.
You can find this file everywhere on your computer.
* Don't Delete Encrypted Files
* Don't Modify Encrypted Files
* Don't Rename Encrypted Files

02

How Ransomware Spreads

(Emails, Phishing, etc.)



INFOSEC
INFORMATION SECURITY SOLUTIONS

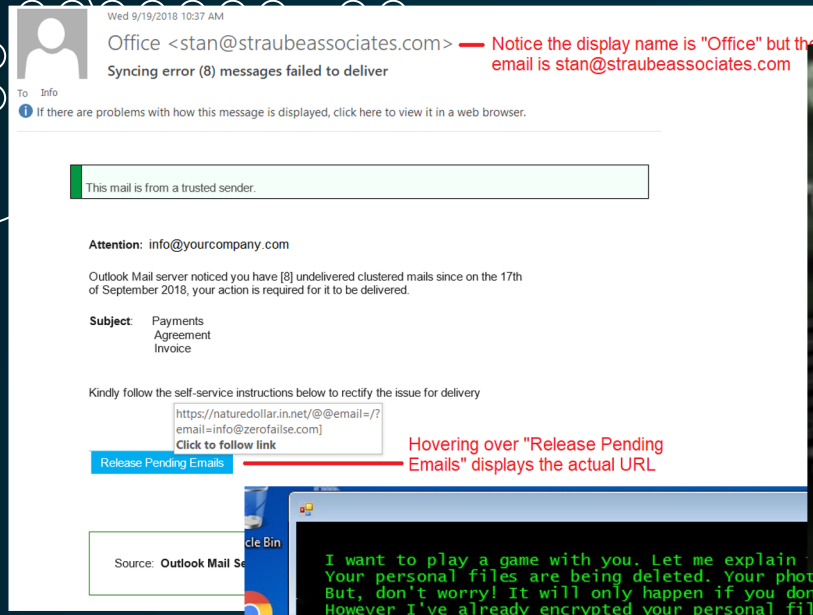
How Ransomware Spreads

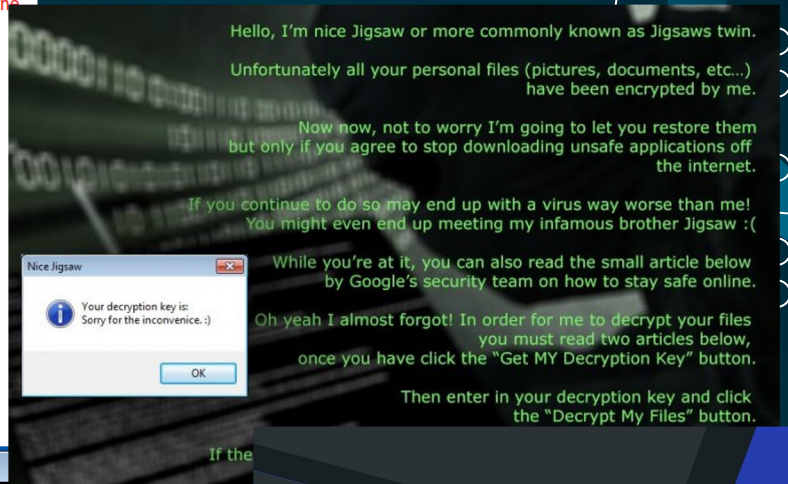
Do you know how ransomware infects your system? Here are common ways:

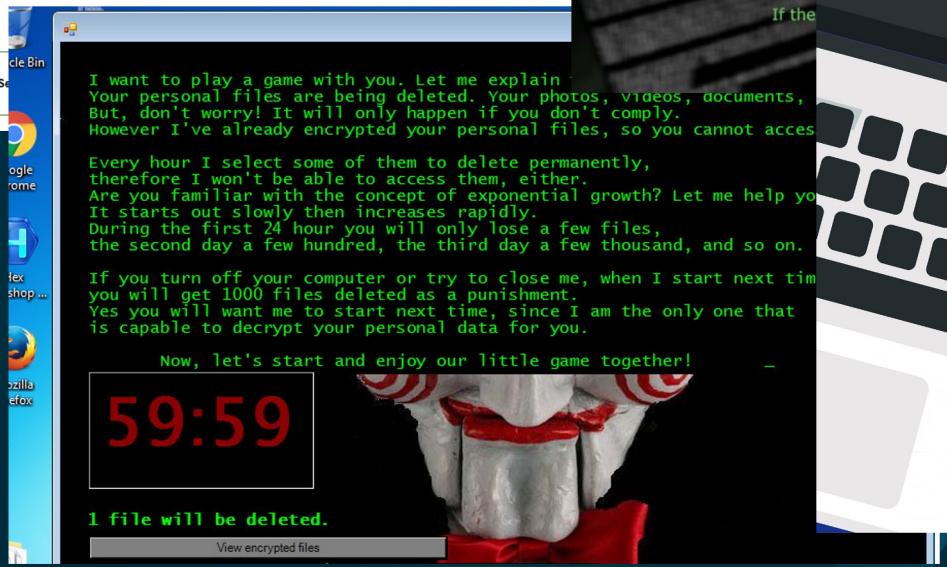
- **Phishing Emails**
- **Malicious Websites**
- **Infected Software**
- **USB Drives**

And the most important thing: Stay vigilant and **avoid opening suspicious emails or links!**

INFOSEC
INFORMATION SECURITY SOLUTIONS





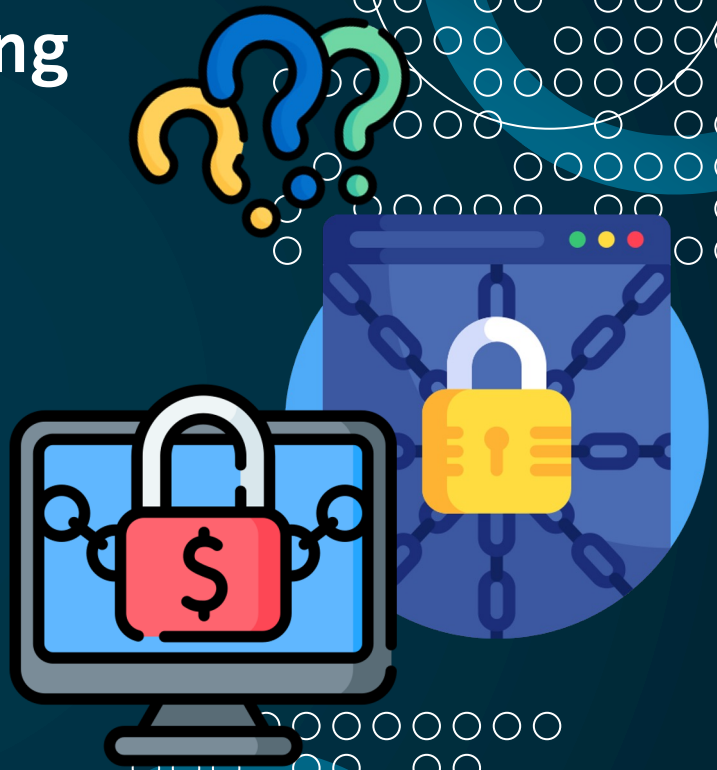


INFOSEC
INFORMATION SECURITY SOLUTIONS

Challenges of Decrypting Ransomware

Do you know how ransomware infects your system? Here are common ways:

- Strong cryptographic algorithms and advanced encryption models (eg. AES, RSA, etc.)
- Decryption without the key is nearly impossible
- Unique keys for each victim



INFOSEC
INFORMATION SECURITY SOLUTIONS

03

The Real Costs of Ransomware Attack

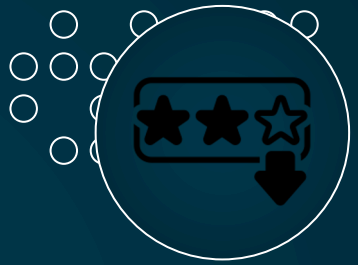
INFOSEC
INFORMATION SECURITY SOLUTIONS

Financial Loss

Ransom payments
Downtime and lost productivity Recovery costs

Data Loss

Permanent loss of critical files
Risk of data corruption or destruction

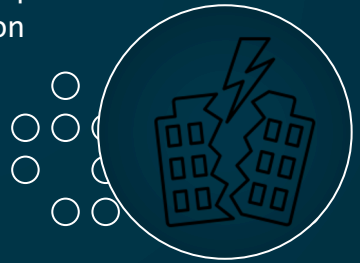


Reputation Damage

Legal consequences due to data breaches

Regulatory Fines

Violations of data protection laws (GDPR, HIPAA, etc.)
Failure to meet compliance standards



Business Disruption

Delayed operations
Potential bankruptcy for small businesses

INFOSEC
INFORMATION SECURITY SOLUTIONS

04

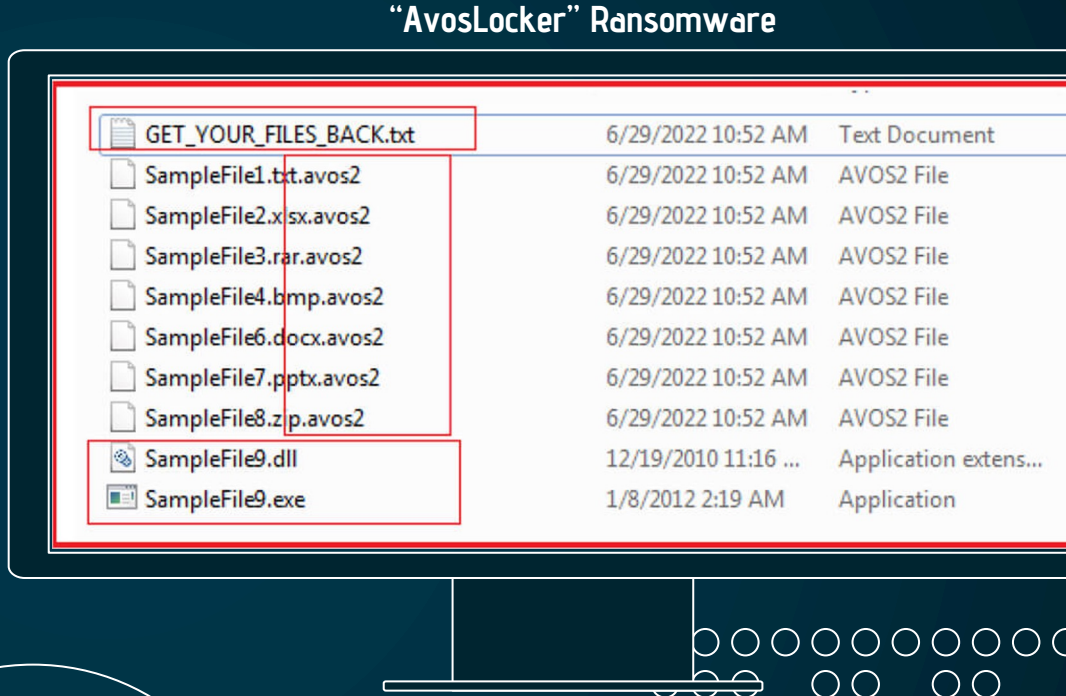
How to Recognize Ransomware

INFOSEC
INFORMATION SECURITY SOLUTIONS

Unusual File Extensions

Files may suddenly have strange or new extensions, like ".encrypted" or ".lock".

For example, a file like **document.pdf** might become **document.pdf.avos.**



INFOSEC
INFORMATION SECURITY SOLUTIONS

Ransom Note

A message appears demanding payment in exchange for decrypting your files.

INFOSEC
INFORMATION SECURITY SOLUTIONS

High CPU Usage

Suspiciously high system resource usage can indicate **encryption processes** happening in the background.

05

Prevention Strategies

INFOSEC
INFORMATION SECURITY SOLUTIONS

HOW TO SECURE YOUR DATA

Regular Backups

Keep frequent backups of your files in offline or cloud storage

Email Awareness

Be cautious of phishing emails.

Update Software

Ensure all software, including operating systems and antivirus, are updated regularly.

Network Segmentation

Isolate critical systems and data from other parts of the network.

INFOSEC
INFORMATION SECURITY SOLUTIONS

06

Fighting Ransomware

INFOSEC
INFORMATION SECURITY SOLUTIONS

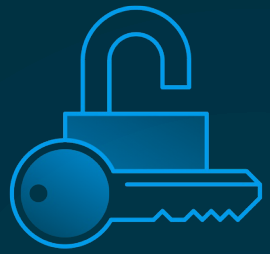
Fighting Ransomware: Solutions and Defense Mechanisms

Bitdefender
Ransomware Remediation

Sophos Intercept X

SentinelOne
Ransomware Rollback

Decrypting Ransomware



- FBI released 7,000 keys to help victims recover from ransomware attacks
- Indonesian hackers encrypted government data but later claimed their actions were intended as a pentest, leading to their apology and promise to provide decryption tools.
- It’s crucial for victims not to delete encrypted files immediately, as recovery may still be possible through free decryption tools or support from initiatives like No More Ransom.

text 144.01 KB

```
#define MODULUS_V   {\
    0xd4,0xa9,0x28,0xc8,0x32,0x9b,0x21,0x3f,\
    0xf0,0x77,0x4a,0xbb,0xd0,0xc6,0x59,0x1a,\
    0xc8,0x2f,0xe5,0xe6,0x17,0x18,0x83,0x79,\
    0xde,0x07,0x1c,0xe9,0xb7,0xb6,0x52,0xd7,\
    0x83,0x80,0xc6,0xc9,0x3b,0x73,0x2b,0x18,\
    0xdc,0xa4,0x4f,0x34,0xe6,0x4d,0x74,0xa0,\
    0x49,0xbe,0x25,0x80,0x86,0xcb,0x27,0x2c,\
    0xa9,0x00,0xc9,0x7a,0x78,0x9e,0x6b,0x9e,\
    0x5e,0xce,0xce,0x60,0xca,0x17,0x1e,0x0b,\
    0x8c,0xd7,0xdd,0x88,0x3d,0x26,0x0f,0x1f,\
    0x40,0x5a,0xb5,0x33,0xb1,0xd0,0xbb,0x00,\
    0x88,0xa1,0xde,0xd1,0xf6,0x76,0xc8,0xdd,\
    0xfd,0x75,0x9e,0x9b,0xa1,0xce,0xcb,0xdd,\
    0xc9,0x0e,0x00,0x38,0x2c,0x6e,0xeb,0x39,\
    0x1e,0x44,0x41,0xbe,0xd6,0x9e,0x74,0x95,\
    0xd2,0x05,0xa6,0xad,0x2f,0xa3,0xc2,0xc9,\
/*Key 0 */\
    0xa3,0xa1,0x68,0x06,0x45,0x46,0x30,0x3e,\
```

Dharma ransomware (.dharma) decryptor

INFOSEC
INFORMATION SECURITY SOLUTIONS

Decrypting Ransomware

- No More Ransom is an initiative launched in July 2016, created to help victims of ransomware recover their files without having to pay the ransom.
- Collaboration between law enforcement agencies, cybersecurity companies, and various organizations. Key partners include *Europol*, the *Dutch National Police*, and cybersecurity companies like *McAfee, Kaspersky, and ESET*.
- The website offers a range of free decryption tools for various types of ransomware.
- In addition to tools, No More Ransom provides educational content to raise awareness about ransomware, prevention tips, and guidance on how to report incidents.

INFOSEC
INFORMATION SECURITY SOLUTIONS

- **Increased Sophistication**
  Ransomware attacks are becoming more advanced, with attackers using AI to bypass defenses and spread more quickly.

- **Ransomware-as-a-Service (RaaS)**
  Cybercriminals are offering ransomware kits to others, making attacks easier to execute and more widespread.

- Targeting Critical Infrastructure: Attacks on healthcare, energy, and government sectors are expected to rise, causing greater disruption and financial damage.

- **Double/Triple Extortion**
  Beyond encrypting files, attackers may steal sensitive data and threaten to leak it, adding pressure to pay the ransom.

- **Cryptocurrency Regulation**
  Increased regulation of cryptocurrencies may impact how easily criminals can collect ransoms in the future.

INFOSEC
INFORMATION SECURITY SOLUTIONS

Any questions?

INFOSEC
INFORMATION SECURITY SOLUTIONS

THANK YOU!

Contact: areg.shmavonyan@infosec.am