



Riešenie kybernetických incidentov pomocou IDS



LADISLAV BAČO

 @MALWARELAB_EU@INFOSEC.EXCHANGE

whoami

Kyberbezpečnosť

- Analýza malvéru a sieťovej komunikácie
- Riešenie incidentov
- Vzdelávanie
- Analytik sieťových infiltrácií, ESET



Agenda

Príprava

Ukážka kybernetického útoku

Riešenie incidentov

Poznatky z praxe

Tipy & triky

Q&A



Životný cyklus riešenia incidentov

Nikdy nekončiaci process

Computer Security Incident Handling Guide, NIST SP 800-61 Rev.2

Incident Response Recommendations, **NIST SP 800-61 Rev.3**

- Zmeny medzi Rev.2 a Rev.3
- Od reaktívneho životného cyklu k neustálemu manažmentu rizík

Príprava

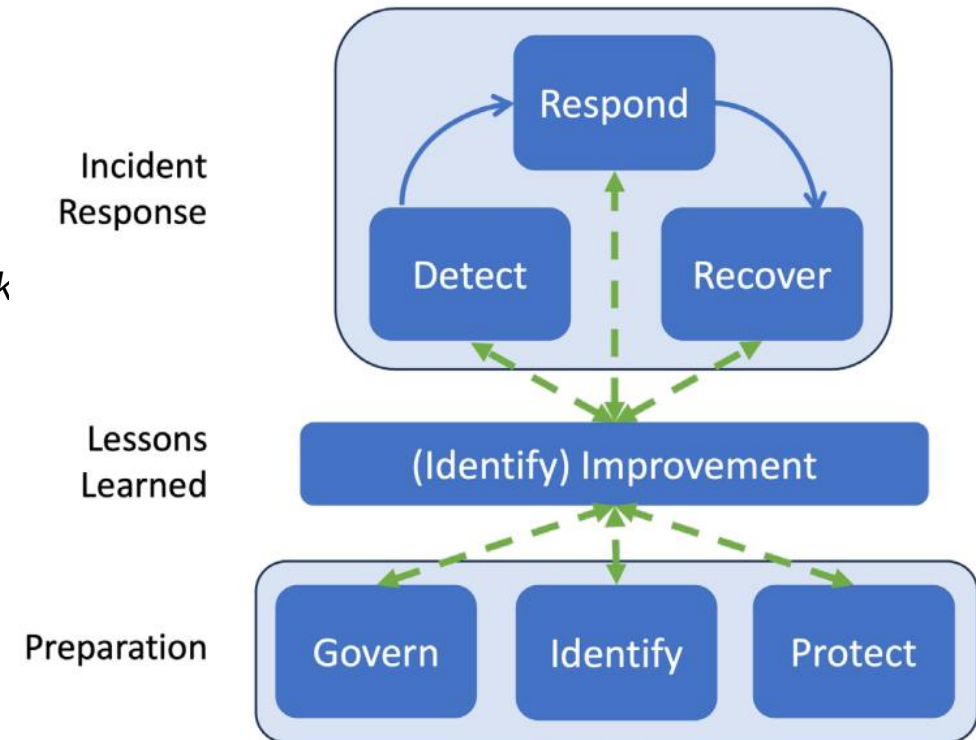
- Riadenie, Identifikácia, Ochrana

Riešenie incidentov

- Detekcia, Riešenie, Obnova

Poučenie z praxe

- Príležitosti na zlepšenie (v každom kroku)



Príprava

Bez logov sme slepí

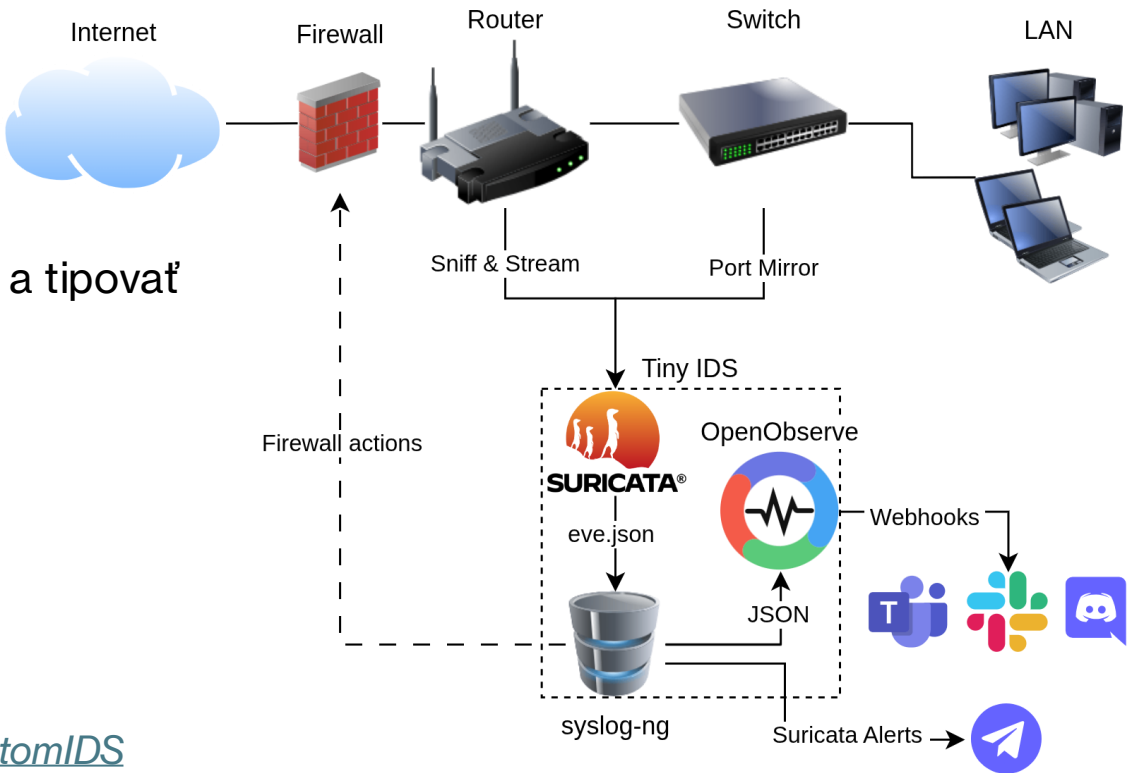
- Bez viditeľnosti do infraštruktúry môžeme iba hádať a tipovať

Home IDS

- Suricata + Pravidlá
- OpenObserve
- Alerty + Notifikácie
- ...

Nasadené v domácej sieti/v labe

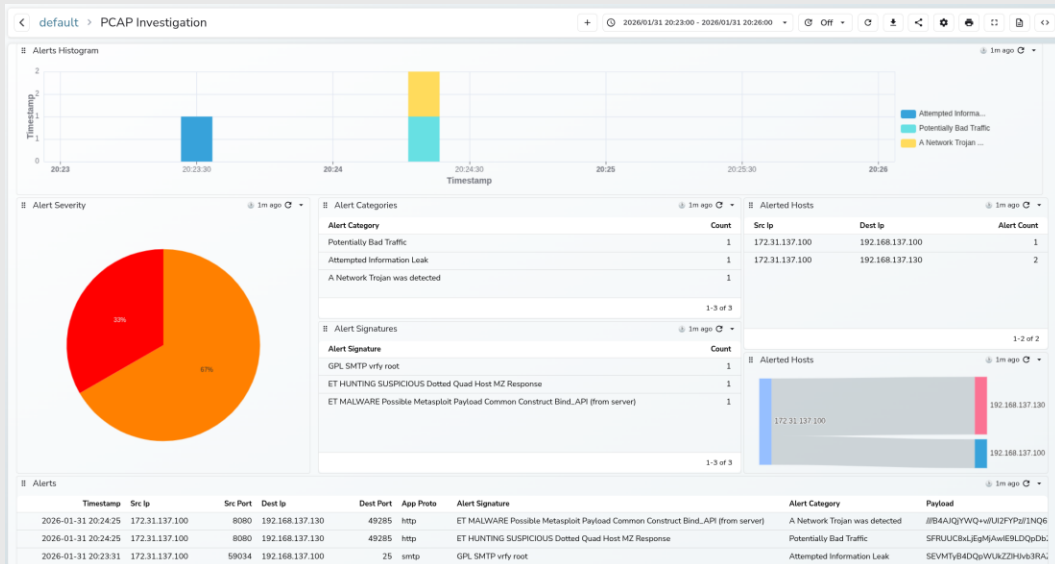
- InstallFest prednáška alebo <https://github.com/laciKE/AtomIDS>



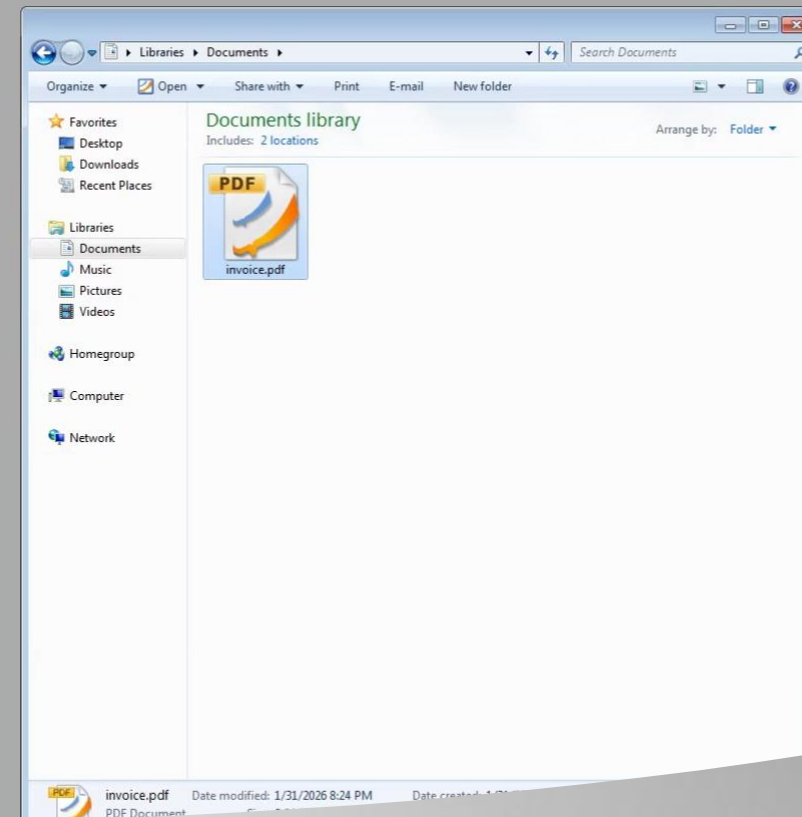
Príprava

Analýza záznamu sieťovej komunikácie

- Užitočné cvičenie
- Analýza ukážkových PCAP súborov
- Reálne incidenty, analýza komunikácie malvéru
- Načítanie logov do Elastic/Open/Search/Observe
- Prepísanie časov hodnotami z PCAP/eve.json
- Políčko @timestamp, _timestamp
- Formát RFC3339
- (V) 2026-03-08T13:06:56.836267+00:00
- (X) 2026-03-08T13:06:56.836267+0000
- Nahratie upraveného eve.json do OpenObserve (curl)
- Staršie logy => ZO_INGEST_ALLOWED_UPTO
- OpenObserve Dashboard pre analýzu PCAP súborov
- <https://github.com/laciKE/AtomIDS/>



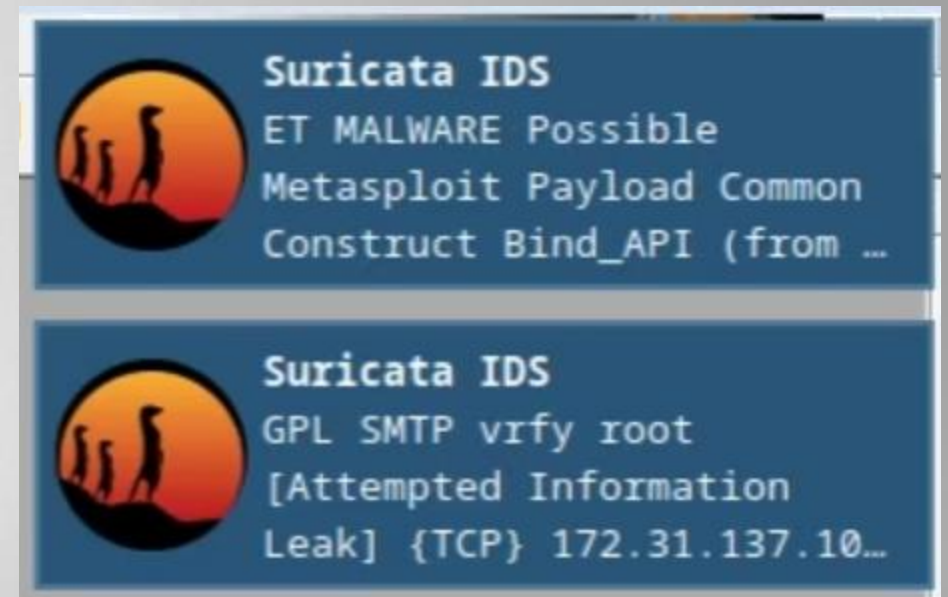
```
System
kali@kali: ~  
msf exploit(multi/handler) > run  
[*] Started HTTP reverse handler on http://172.31.137.100:8080  
[!] http://172.31.137.100:8080 handling request from 192.168.137.130; (UUID: k  
uhrzcjn) Without a database connected that payload UUID tracking will not work  
!  
[*] http://172.31.137.100:8080 handling request from 192.168.137.130; (UUID: k  
uhrzcjn) Staging x86 payload (190044 bytes) ...  
[!] http://172.31.137.100:8080 handling request from 192.168.137.130; (UUID: k  
uhrzcjn) Without a database connected that payload UUID tracking will not work  
!  
[*] Meterpreter session 4 opened (172.31.137.100:8080 → 192.168.137.130:49285  
) at 2026-01-31 21:24:24 +0100  
  
meterpreter > |
```



Ukážka kybernetického útoku

Detekcia

- Telegram/Discord notifikácie s alertmi zo Suricaty
- Analýza alertov
 - Alerts Dashboard
- Zamerajme sa na **5W**:
 - **Who** (Kto)
 - **What** (Čo)
 - **When** (Kedy)
 - **Where** (Kde)
 - **Why** (Prečo)



Aktuálny stav: Alerty

Who:

- Útočník: 172.31.137.100

What:

- Enumerácia emailov
- Stiahnutie EXE súboru
- Network Trojan Payload

When:

- 2026-01-31 20:23:30 – 20:24:45

Where:

- Kompromitované PC: 192.168.137.130
- Mailserver: 192.168.137.100

Why?

Alert Categories		12m ago	
Alert Category	Count		
Potentially Bad Traffic	1		
Attempted Information Leak	1		
A Network Trojan was detected	1		
		1-3 of 3	

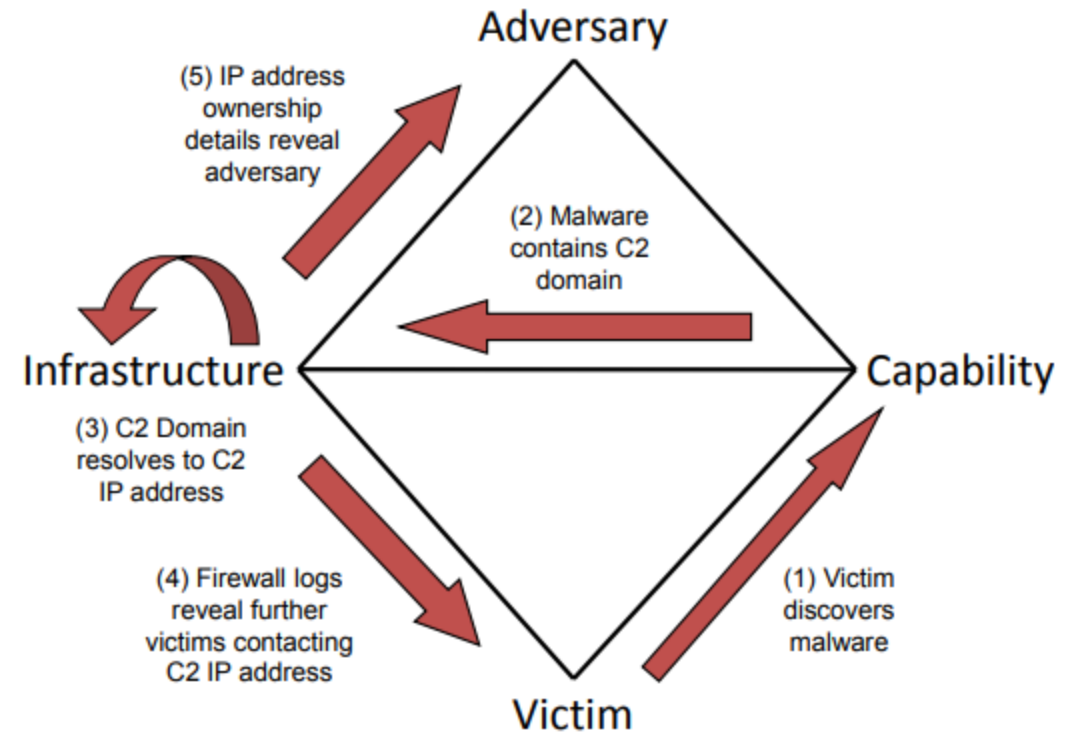
Alert Signatures		12m ago	
Alert Signature	Count		
GPL SMTP vrfy root	1		
ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	1		
ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	1		
		1-3 of 3	

Alerted Hosts			12m ago	
Src Ip	Dest Ip	Alert Count		
172.31.137.100	192.168.137.100	1		
172.31.137.100	192.168.137.130	2		
			1-2 of 2	

Alerted Hosts			12m ago	
				
			1-2 of 2	

Intermezzo: Analytické pivotovanie

- **Diamond Model of Intrusion Analysis**
- Objavovanie súvisiacich elementov, napr.:
 - Od obeti ku nástrojom a technikám
 - Od nástrojov ku infraštruktúre
 - Od infraštruktúry k ďalším obetiam
 - Od infraštruktúry k útočníkovi



Source: https://threatconnect.com/wp-content/uploads/The_Diamond_Model_of_Intrusion_Analysis.pdf

Súvislosti

- **Network Flows Dashboard**
 - Najväčší kecáľkovia
 - Porty/protokoly
 - Dlhé spojenia
 - Mnoho udalostí
 - Kontrola pomocou VirusTotal
- **Analýza logov**
 - Community ID
 - točnickova IP adresa
- **Email Dashboard**

Top Downloaders		7m ago
Src Ip	Flow Bytes Toserver	
192.168.137.130	2.0MB	

Top Uploaders		8m ago
Src Ip	Flow Bytes Toserver	
192.168.137.130	184.3KB	

Long Sessions								
Src Ip	Src Port	Dest Ip	Dest Port	Proto	Flow Age	Flow State	Flow Bytes Toclient	Flow Bytes Toserver
192.168.137.130	49287	172.31.137.100	8080	TCP	54	established	1449001	90910

timestamp (Europe/Bratislava)	src_ip	src_port	dest_ip	dest_port	proto	event_type	http_url
> 2026-01-31 20:25:51.395	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:49.991	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:48.681	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:47.480	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:46.372	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:45.358	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:45.264	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:45.171	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:45.093	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/
> 2026-01-31 20:25:45.030	192.168.137.130	49287	172.31.137.100	8080	TCP	http	/H7VvdEdtU9r6JMc1r1qi0QVVIbcshpB0-Y-5meCuHJXdC-xf/

> 2026-01-31 20:24:25.674	172.31.137.100	8080	192.168.137.130	49286	TCP	fileinfo
> 2026-01-31 20:24:25.609	172.31.137.100	8080	192.168.137.130	49285	TCP	alert
> 2026-01-31 20:24:25.603	172.31.137.100	8080	192.168.137.130	49285	TCP	fileinfo
> 2026-01-31 20:24:25.594	172.31.137.100	8080	192.168.137.130	49285	TCP	alert
> 2026-01-31 20:24:08.569	172.31.137.100	34444	192.168.137.100	25	TCP	smtp
> 2026-01-31 20:24:03.090	172.31.137.100	34444	192.168.137.100	25	TCP	smtp
> 2026-01-31 20:24:03.086	172.31.137.100	34444	192.168.137.100	25	TCP	fileinfo

Emails											now
Timestamp	Src Ip	Src Port	Dest Ip	Dest Port	Smtpl Helo	Smtpl Mail From	Smtpl Rcpt To	Email From	Email To	Email Status	Email Attachment
2026-01-31 20:24:08	172.31.137.100	34444	192.168.137.100	25	[172.31.137.100]						
2026-01-31 20:24:03	172.31.137.100	34444	192.168.137.100	25	[172.31.137.100]	<john@evil.local>	[<dave@demo.local>]	John Doe <john@evil.local>	[<dave@demo.local>]	PARSE_DONE	[\"invoice.pdf\"]

Aktuálny stav: NetFlow a Udalosti

Who:

- Útočník: 172.31.137.100

What:

- Enumerácia emailov
- Email s prílohou invoice.pdf
- Stiahnutie EXE programu
- Network Trojan
Command&Control

When:

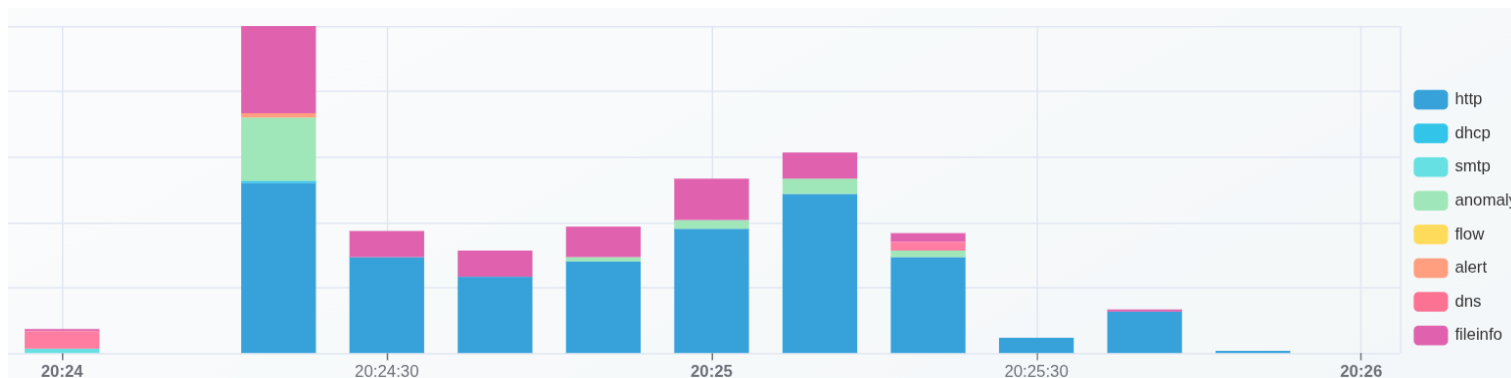
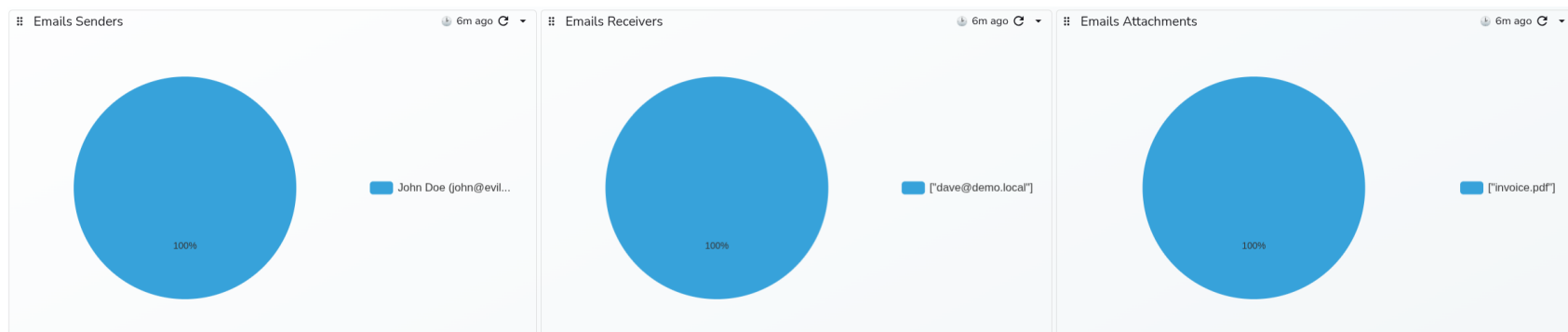
- 2026-01-31 20:23:30 – 20:25:51

Where:

- Kompromitované PC: 192.168.137.130
- Mailserver: 192.168.137.100

Why

- Infikovaná emailová príloha?



Aktuálny stav: Forenzná hypotéza

Enumerácia emailových účtov

- Nájdenie emailovej adresy obete

Odoslanie emailu obeti

- SMTP od útočníka na mailserver

Žiadne POP3/IMAP medzi mailserverom a obeťou

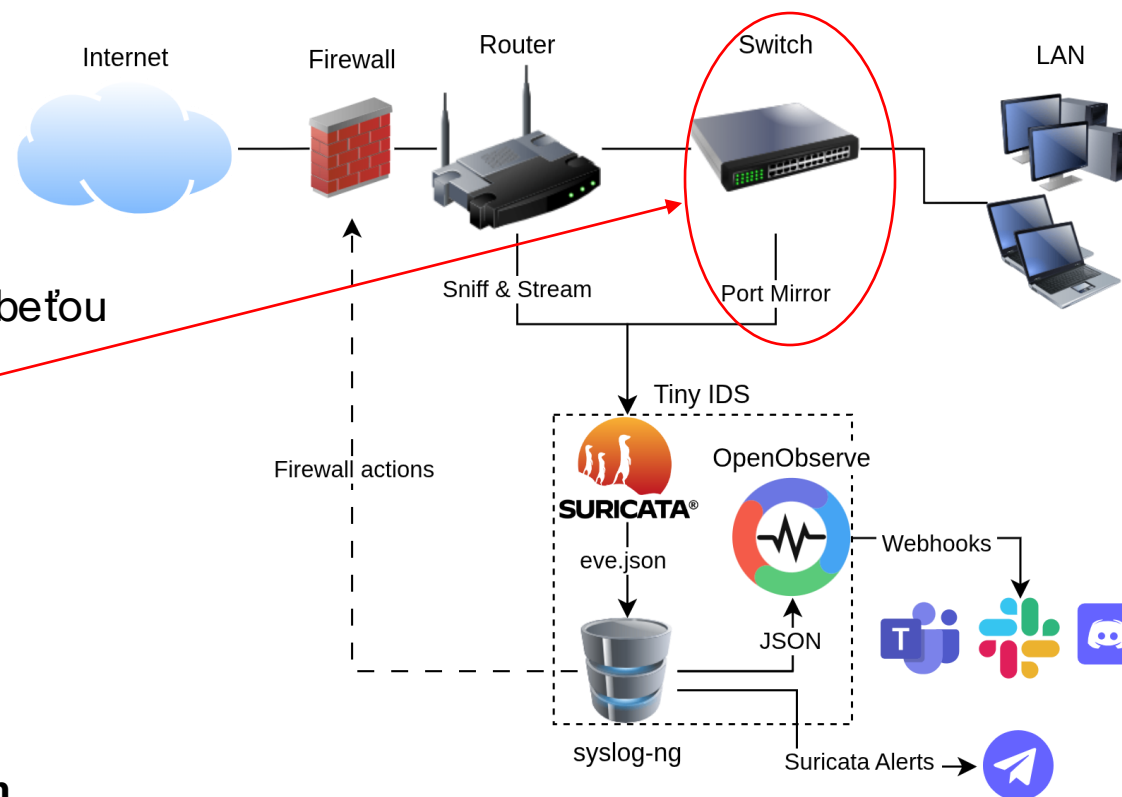
- Prečo?
 - Slepé miesto, medzera vo viditeľnosti
- Poučenie z praxe
 - Zlepšiť zber dát
 - Zlepšiť umiestnenie senzora

Obeť otvorila infikovaná prílohu v emaili

- Invoice.pdf

Obeť stiahla škodlivý EXE súbor s trjským koňom

Trójsky kôň nadviazal Command&Control komunikáciu s útočníkom



Ďalšie kroky: Analýza a "response"

Analýza kompromitovaného PC a mailservera

- Skenovanie na malvér
- Analýza logov OS
 - Logy spúšťaných procesov na PC
 - Windows security logs event id 4688
 - Sysmon event id 1
 - ***Ale nič z toho nemáme***
- Logy z mailservera
 - Potvrdenie že obeť stiahla email
 - Ďalší adresáti podozrivého emailu?

- Nezaznamenaná žiadna ďalšia škodlivá aktivita
 - Žiadne ďalšie sieťové spojenia do/od útočníka alebo obete
- Izolácia kompromitovaného PC
- Zablokovanie útočníka na firewallle
- Fixnutie slepého miesta

Analýza EXE súboru a emailovej prílohy

Čo ak... povolíme **ukladanie súborov**?

- `outputs.file-store.enabled`
- `outputs.file-store.force-filestore`

Upravíme hbkú inspekcie na >100kB

- `outputs.file-store.stream-depth`
- `app-layer.protocols.http.libhttp.default-config.response-body-limit`
- `app-layer.protocols.http.libhttp.default-config.request-body-limit`

- Analýza EXE súboru
 - Skenovanie na malvér
 - Extrakcia textových reťazcov
- Analýza Invoice.pdf
 - Metadáta: exiftool
 - Dáta: xxd
- Na kompromitovanom PC:
 - Kontrola SysInternals Autoruns
 - Kontrola nedávno modifikovaných súborov

Aktuálny stav: EXE a Invoice.pdf

Metasploit EXE

- Meterpreter Agent
- Textové reťazce:
- Známe patterny Meterpretera
- User Agent
- URL C&C servera

```
http://172.31.137.100:8080/H7VvdEdtU9rGJMcLr1qi0QYVIBCshpB0-Y-5meCuHJXdC-xcf/
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.2903.86
```

Invoice.pdf

- Metadáta: Názov obsahuje mnoho medzier a exploit
- Dáta: Egghunter + Egg

```
File Type      : PDF
File Type Extension : pdf
MIME Type      : application/pdf
PDF Version    : 1.4
Linearized     : No
Page Count     : 1
Language       : en-US
Title          : Free torrent sites
```

ZAKjAa\AaATA²₃₀₃TaYAlAIAlAIAlAIAlAIAlAIAlAIAlAI
IAIxAQADAZABARALAYAlAQAlAQAlAhAAAZlAlAlAJ11AlAlABABABOl1AlOIAl

Poučenie z praxe

Monitoring sieťovej komunikácie je užitočný



Sieťové IDS nám môže pomôcť nájsť škodlivé udalosti aj bez bezpečnostných riešení nainštalovaných na počítačoch



Suricata logy môžu pomôcť s analýzou a riešením incidentov



Dobré umiestnenie senzorov je dôležité

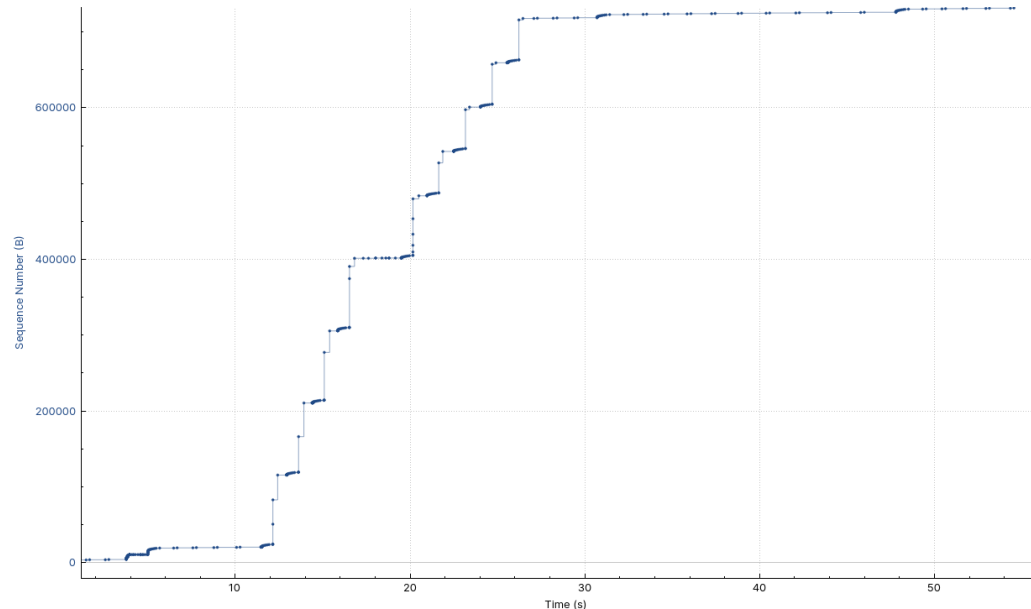
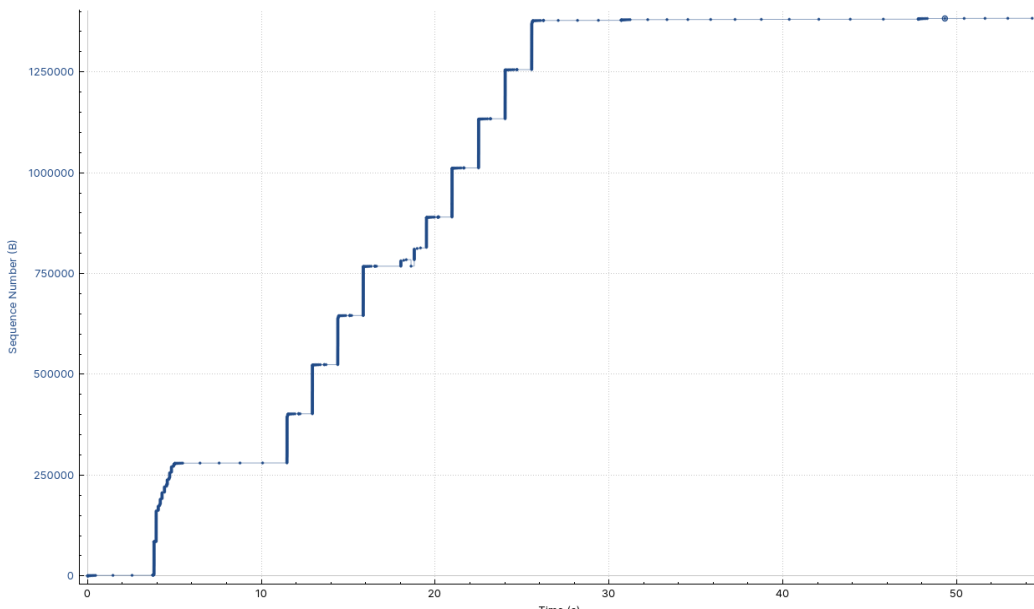
Tipy & Triky

- Ukladanie súborov je mocný nástroj
 - Pravidlá na ukladanie podozrivých súborov
- Príležitosť na automatizáciu:
 - Ukladať všetko, skenovať na malvér a mazať čisté súbory
- Denné aktualizácie pravidiel Suricaty
- Nastaviť Log retention v OpenObserve pre každý Stream (Index)
- Samostatný Stream (Index) pre analýzu PCAP súborov

Tipy & Triky

- **Analýza šifrovanej komunikácie**
 - TLS rozšírenia a vlastnosti
 - SNI, Certificate info, JA3 a JA4 odtlačky
 - Pozrite sa na "tvar" sieťovej komunikácie
 - Počítadlá packetov a bytov
- **Pomoc AI pri analýze**

```
▼ tls_client_alpn:["h2","http/1.1"],  
▼ tls_ja3_hash:1383cbd0529323993c3207b725bf97d8,  
▼ tls_ja3_string:771,4865-4866-4867-49195-49199-49  
▼ tls_ja3s_hash:2253c82f03b621c5144709b393fde2c9,  
▼ tls_ja3s_string:771,4866,43-51-41,  
▼ tls_ja4:t13d1516h2_8daaf6152771_9b887d9acb53,  
▼ tls_sni:www.eicar.org,  
▼ tls_version:TLS 1.3
```



Záver

Domáci IDS systém na detekciu a analýzu incidentov

GitHub repozitár

- <https://github.com/laciKE/AtomIDS>
- Návod, konfiguračné súbory, openrc služby
- OpenObserve Dashboard
- eve.json z ukážkového útoku
- 3D krabička pre Dell Wyse 3040 + TL-SG105E ;:-)

Kontakt

- Mastodon: [@malwarelab_eu@infosec.exchange](https://infosec.exchange/@malwarelab_eu)
- X: [@ladislav_b](https://twitter.com/ladislav_b), [@malwarelab_eu](https://twitter.com/malwarelab_eu)
- Web: <https://malwarelab.eu>

