

BEST

-

Laboratorium 2

Paweł Murdzek, 310850

Politechnika Warszawska

25 maja 2025

Spis treści

1. Wstęp	2
2. Zadania	2
2.1. How many packets does the capture have?	2
2.2. At what time was the first packet captured?	2
2.3. What is the duration of the capture?	2
2.4. What is the most active computer at the link level?	3
2.5. Manufacturer of the NIC of the most active system at the link level?	3
2.6. Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?	3
2.7. How many computers in the organization are involved in the capture?	4
2.8. What is the name of the most active computer at the network level?	4
2.9. What is the IP of the organization's DNS server?	5
2.10. What domain is the victim asking about in packet 204?	5
2.11. What is the IP of the domain in the previous question?	5
2.12. Indicate the country to which the IP in the previous section belongs.	5
2.13. What operating system does the victim's computer run?	5
2.14. What is the name of the malicious file downloaded by the accountant?	6
2.15. What is the MD5 hash of the downloaded file?	6
2.16. What software runs the webserver that hosts the malware?	6
2.17. What is the public IP of the victim's computer?	6
2.18. In which country is the email server to which the stolen information is sent?	7
2.19. What software runs the email server to which the stolen data is sent?	7
2.20. To which email account is the stolen information sent?	7
2.21. What is the password used by the malware to send the email?	7
2.22. Which malware variant exfiltrated the data?	7
2.23. What are the bankofamerica access credentials?	8
2.24. Every how many minutes does the collected data get exfiltrated?	8
3. Podsumowanie	8

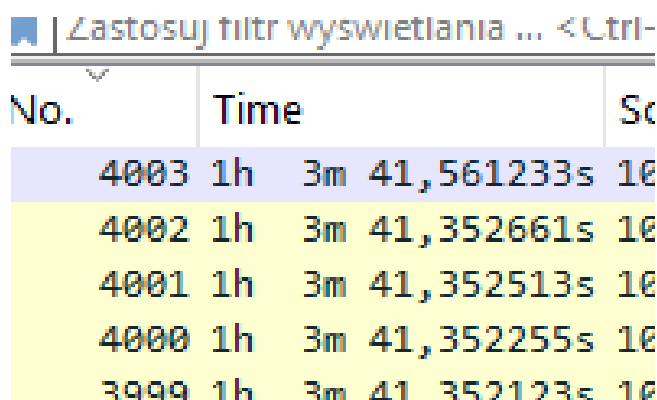
1. Wstęp

Niniejsze sprawozdanie przedstawia wyniki analizy ruchu sieciowego, zrealizowanej w ramach wyzwania Blue Team CTF platformy CyberDefenders. Głównym celem analizy było zidentyfikowanie i scharakteryzowanie incydentu bezpieczeństwa, w szczególności infekcji złośliwym oprogramowaniem typu infostealer/keylogger. Zadanie obejmowało szczegółowe badanie przechwyconych pakietów sieciowych w celu ustalenia kluczowych wskaźników kompromitacji, takich jak nazwa złośliwego pliku, jego skrót MD5, wykorzystane serwery i metody eksfiltracji danych. Analiza miała na celu dostarczenie kompleksowego obrazu ataku oraz zidentyfikowanie zagrożeń związanych z oprogramowaniem HawkEye Keylogger.

2. Zadania

2.1. How many packets does the capture have?

4003

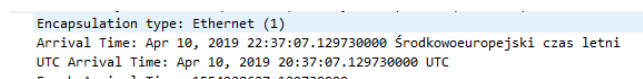


No.	Time	Size
4003	1h 3m 41,561233s	10
4002	1h 3m 41,352661s	10
4001	1h 3m 41,352513s	10
4000	1h 3m 41,352255s	10
3999	1h 3m 41,352123s	10

Rysunek 1: Capture packets

2.2. At what time was the first packet captured?

Arrival Time: Apr 10, 2019 22:37:07.129730000 Środkowoeuropejski czas letni



Encapsulation type: Ethernet (1)
Arrival Time: Apr 10, 2019 22:37:07.129730000 Środkowoeuropejski czas letni
UTC Arrival Time: Apr 10, 2019 20:37:07.129730000 UTC

Rysunek 2: First packet capture time

2.3. What is the duration of the capture?

2019-04-19 20:37:07 UTC 01:03:41

Zastosuj filtr wyświetlania ... <Ctrl-

No.	Time	Sc
4003	1h 3m 41,561233s	10
4002	1h 3m 41,352661s	10
4001	1h 3m 41,352513s	10
4000	1h 3m 41,352255s	10
3999	1h 3m 41,352123s	10

Rysunek 3: Capture duration

2.4. What is the most active computer at the link level?

Statystyki > Punkty krańcowe 00:08:02:1c:47:ae

Ethernet - 7	IPv4 - 12	IPv6	TCP - 48	UDP - 58		
Adres	Pakiety	Bajty	Wyslane pakiety	Bajty Tx	Pakiety Rx	Bajty Rx
00:08:02:1c:47:ae	4003	2 MB	1993	212 kB	2010	2 MB
20:e5:2a:b6:93:f1	3352	2 MB	1776	2 MB	1576	110 kB
a4:1f:72:c2:09:6a	513	114 kB	234	46 kB	279	68 kB
01:00:5e:00:00:16	23	1 kB	0	0 bajty	23	1 kB
01:00:5e:00:00:fc	10	750 bajty	0	0 bajty	10	750 bajty
01:00:5e:7f:ff:fa	74	29 kB	0	0 bajty	74	29 kB
ff:ff:ff:ff:ff:ff	31	4 kB	0	0 bajty	31	4 kB

Rysunek 4: Most active computer at link level

2.5. Manufacturer of the NIC of the most active system at the link level?

<https://maclookup.app/search/result?mac=00:08:02:1c:47:ae>

Hewlett-Packard

Hewlett Packard

Vendor Details History

MAC address prefix **00:08:02** is registered to **Hewlett Packard**, located at 20555 State Highway 249Houston TX 77070US.

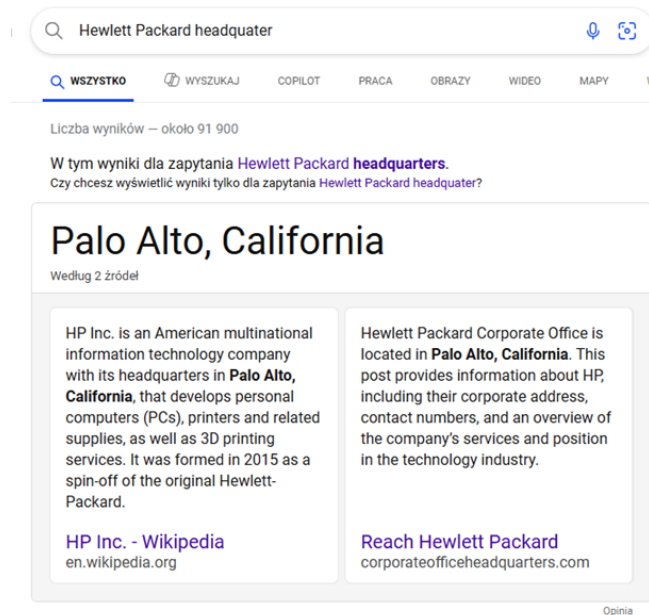
This registration is classified as **MA-L** (Mac Address Block Large) containing approximately 16 million MAC addresses

The prefix was initially registered on **24 October 2001**, with the most recent update made on **17 November 2015**.

Rysunek 5: NIC manufacturer

2.6. Where is the headquarter of the company that manufactured the NIC of the most active computer at the link level?

Palo Alto



Rysunek 6: Headquarters of NIC manufacturer

2.7. How many computers in the organization are involved in the capture?

The organization works with private addressing and netmask /24. IPv4 > Source and Destination Adresses 10.4.10.255 to jest adres broadcastowy, więc nie liczymy go. Poprawna odpowiedź to 3.

Ethernet · 7	IPv4 · 12	IPv6	TCP · 48	UDP · 58	
Adres	Pakiety	Bajty	Całkowita liczba pakietów		Filtrowane procentów
10.4.10.2	42	5 kB	42		100.0%
10.4.10.4	513	114 kB	513		100.0%
10.4.10.132	2227	258 kB	4003		55.6%
10.4.10.255	30	3 kB	30		100.0%
23.229.162.69	119	26 kB	280		42.5%
66.171.248.178	35	2 kB	63		55.5%
216.58.193.131	9	3 kB	20		45.0%
217.182.138.150	1371	74 kB	2947		46.5%
224.0.0.22	23	1 kB	23		100.0%
224.0.0.252	10	750 bajty	10		100.0%
239.255.255.250	74	29 kB	74		100.0%
255.255.255.255	1	342 bajty	1		100.0%

Rysunek 7: Computers involved in capture

2.8. What is the name of the most active computer at the network level?

Przy DHCP, host rozgłasza swoje imię, jeśli odczytamy informacje w momencie ich nadania, możemy odczytać adres sprzętu: Beijing-5cd1-PC

Rysunek 8: Most active computer at network level

2.9. What is the IP of the organization's DNS server?

10.4.10.4

[illegible]

Rysunek 9: Organization's DNS server IP

2.10. What domain is the victim asking about in packet 204?

proforma-invoices.com

203	46,6375565	10.4.10.132	10.4.10.255	NBNS	92 Name query NB WPAD(00)
204	46,6612875	10.4.10.132	10.4.10.4	DNS	81 Standard query 0xa002 A proforma-invoices.com
205	46,6612875	10.4.10.132	10.4.10.255	NBNS	82 Standard query 0xa002 A proforma-invoices.com

Rysunek 10: Domain victim is asking about

2.11. What is the IP of the domain in the previous question?

217.182.138.150

204 46,6612876	10.4.10.132	10.4.10.4	DNS	81 Standard query 0xa002 A proforma-invoices.com
206 47,6472891	10.4.10.4	10.4.10.132	DNS	97 Standard query response 0xa002 A proforma-invoices.com A 217.182.138.150

Rysunek 11: IP of the domain

2.12. Indicate the country to which the IP in the previous section belongs.

<https://whatismyipaddress.com/ip/217.182.138.150#:~:text=IP%20data%20from%20IP2Location.%20Location%3A%20Roubaix%2C%20France%20-,IP%20address%20allocated%20to%20OVH%20SAS.%20Learn%20more.France>

2.13. What operating system does the victim's computer run?

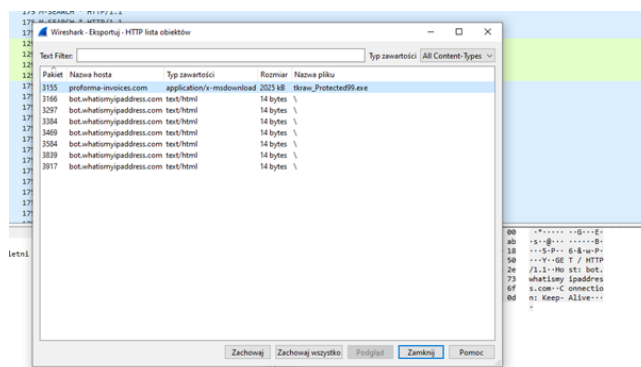
Windows NT 6.1

```
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WC  
Host: nonforma-invoices.com\r\n
```

Rysunek 12: Victim's operating system

2.14. What is the name of the malicious file downloaded by the accountant?

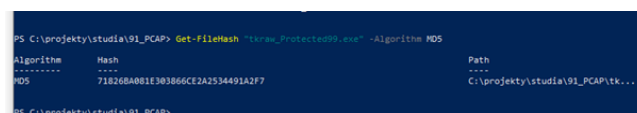
Plik > eksportuj pakiety > http tkraw_Protected99.exe



Rysunek 13: Name of malicious file

2.15. What is the MD5 hash of the downloaded file?

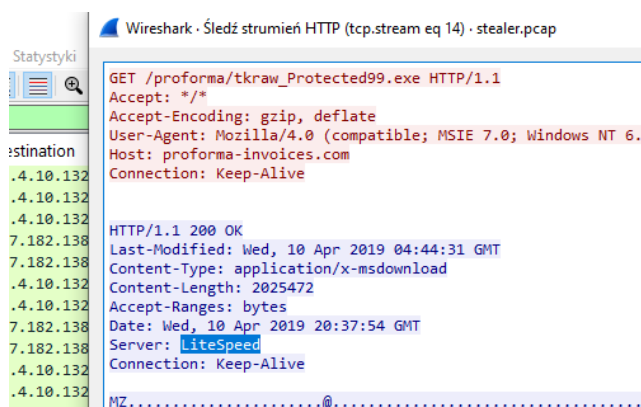
Podążaj > HTTP Eksportuj obiekty > http > pobierz Zdehashowanie za pomocą PS: Get-FileHash "tkraw_Protected99.exe" -Algorithm MD5 71826BA081E303866CE2A2534491A2F7



Rysunek 14: MD5 hash of downloaded file

2.16. What software runs the webserver that hosts the malware?

LiteSpeed Podążaj > strumień HTTP



Rysunek 15: Webserver software

2.17. What is the public IP of the victim's computer?

173.66.146.112 Tuż po zapytaniu bot.whatismyipadress.com mamy odpowiedź na to pytanie.

3150	Sm	8.542556	18.4.18.132	18.4.18.4	SMTP	25 Standard query R=US A Use=ubtwinlogistics.com
3151	Sm	8.576426	18.4.18.4	18.4.18.132	SMTP	381 Standard query R=US A Use=ubtwinlogistics.com
3152	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3153	Sm	8.580794	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [FIN, ACK] Seq=64248 Win=0 Len=0
3154	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [ACK] Seq=64248 Win=0 Len=0
3155	Sm	8.580804	18.4.18.132	60.171.248.178	SMTP	34 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3156	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3157	Sm	8.580804	60.171.248.178	18.4.18.132	SMTP	34 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3158	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3159	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3160	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3161	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3162	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3163	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3164	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3165	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3166	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3167	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3168	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3169	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3170	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3171	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3172	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3173	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3174	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3175	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3176	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3177	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0

Rysunek 16: Victim's public IP

2.18. In which country is the email server to which the stolen information is sent?

United States 173.66.146.112 IP Address Details - IPinfo.io Analyzing the first extraction of information.

2.19. What software runs the email server to which the stolen data is sent?

Przy pierwszej odpowiedzi w protokole SMTP – Simple Mail Transfer Protocol, możemy w szczegółach przeczytać informacje o oprogramowaniu.

3177	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3178	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3179	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3180	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3181	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3182	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3183	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3184	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3185	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3186	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3187	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3188	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3189	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3190	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0

Rysunek 17: Email server software

2.20. To which email account is the stolen information sent?

sales.del@macwinlogistics.in

3186	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3187	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3188	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3189	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3190	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0

Rysunek 18: Email account for stolen information

2.21. What is the password used by the malware to send the email?

Szukamy logowania: Możemy zdekodować wartość za pomocą Base64 Sales@23

3186	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3187	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3188	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0
3189	Sm	8.580804	60.171.248.178	18.4.18.132	TCP	18 80 → 40285 [ACK] Seq=64248 Win=0 Len=0
3190	Sm	8.580804	18.4.18.132	60.171.248.178	TCP	60 40285 → 80 [FIN, ACK] Seq=64248 Win=0 Len=0

Rysunek 19: Password used by malware

2.22. Which malware variant exfiltrated the data?

Follow > TCP stream. Mamy wartości maila: Zakodowane w base64 Po zdekodowaniu nagłówek: HawkEye Keylogger - Reborn v9 Passwords Logs



Rysunek 20: Malware variant

2.23. What are the bankofamerica access credentials?

(username:password) Po zdekodowaniu możemy wyszukać bankofamerica (ctrl+f) roman.mcguire:P@ssw0rd\$

2.24. Every how many minutes does the collected data get exfiltrated?

Co 10 minut. (filtr smtp)

3. Podsumowanie

Przeprowadzona analiza ruchu sieciowego zidentyfikowała obecność złośliwego oprogramowania HawkEye Keylogger - Reborn v9 w środowisku organizacji. Incydent rozpoczął się od pobrania pliku tkraw_Protected99.exe z serwera hostującego złośliwe oprogramowanie, działającego na oprogramowaniu LiteSpeed. Analiza pakietów ujawniła, że najbardziej aktywnym komputerem na poziomie łącza był system o adresie MAC 00:08:02:1c:47:ae, wyprodukowany przez Hewlett-Packard z siedzibą w Palo Alto. Komputer ofiary, z systemem operacyjnym Windows NT 6.1 i publicznym adresem IP 173.66.146.112, był aktywnie zaangażowany w incydent.

Kluczowe ustalenia obejmują:

- **Nazwa złośliwego pliku:** tkraw_Protected99.exe
- **Skrót MD5:** 71826BA081E303866CE2A2534491A2F7
- **Zidentyfikowane oprogramowanie:** HawkEye Keylogger - Reborn v9
- **Metoda eksfiltracji:** Dane były wysyłane co 10 minut na konto e-mail sales.del@macwinlogistics.in za pośrednictwem serwera pocztowego Exim 4.91 #1, zlokalizowanego w Stanach Zjednoczonych. Wykorzystane hasło to Sales@23.
- **Skradzione dane:** Wśród eksfiltrowanych danych znaleziono dane uwierzytelniające do Bank of America: roman.mcguire:P@ssw0rd\$.

Analiza potwierdza, że HawkEye Keylogger skutecznie gromadzi poufne informacje, takie jak dane uwierzytelniające, i eksfiltruje je do kontrolowanego przez atakującego serwera pocztowego. Łączna liczba pakietów wynosiła 4003, a czas trwania przechwytywania wynosił 01:03:41. Te ustalenia są kluczowe dla działań reagowania na incydenty i wzmocnienia pozycji bezpieczeństwa.