Paweł Murdzek,

Piotr Szewczyk,

BEST Lab2

1. **How many packets does the capture have?**

4003

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. **At what time was the first packet captured?**

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

2019-04-19 20:37:07 UTC

1. **What is the duration of the capture?**

01:03:41

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. **What is the most active computer at the link level?**

Statystyki > Punkty krańcowe

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

00:08:02:1c:47:ae

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

[**MAC address 00:08:02 | MAC Address Lookup**](https://maclookup.app/search/result?mac=00:08:02:1c:47:ae)Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Hewlett-Packard

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

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Palo Alto

1. **The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?**

IPv4 > Source and Destination Adressess

Obraz zawierający tekst, zrzut ekranu, numer, wyświetlacz

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

10.4.10.255 to jest adres broadcastowy, więc nie liczymy go. Poprawna odpowiedź to 3.

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

Przy DHCP, host rozgłasza swoje imię, jeśli odczytamy informacje przy momencie ich nadania, możemy odczytać adres sprzętu:  
Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Beijing-5cd1-PC

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

10.4.10.4

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

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

proforma-invoices.com



1. **What is the IP of the domain in the previous question?**



217.182.138.150

1. **Indicate the country to which the IP in the previous section belongs.**

[**IP Address Lookup for 217.182.138.150 in Roubaix, France**](https://whatismyipaddress.com/ip/217.182.138.150)

France

1. **What operating system does the victim’s computer run?**



Windows NT 6.1

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

Plik > eksportuj pakiety > http

Obraz zawierający tekst, oprogramowanie, Ikona komputerowa, komputer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

tkraw\_Protected99.exe

1. **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

Obraz zawierający tekst, Czcionka, zrzut ekranu, Jaskrawoniebieski

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. **What software runs the webserver that hosts the malware?**

LiteSpeed

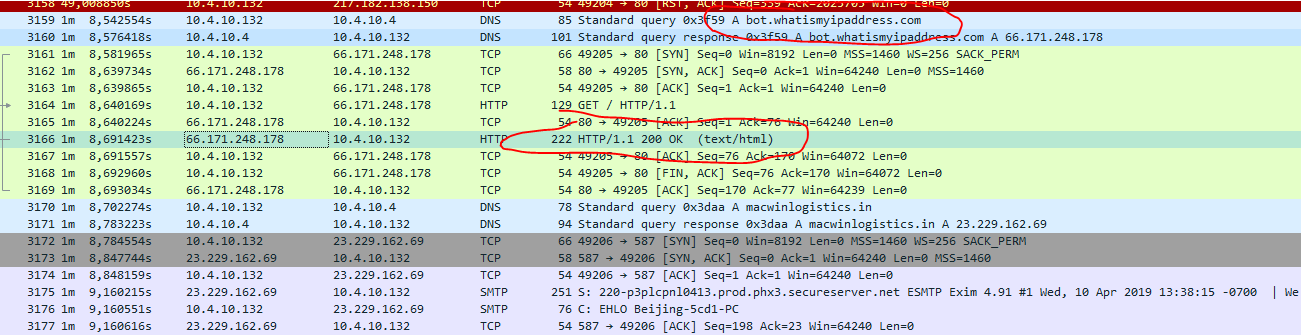
Podążaj > strumień HTTP

Obraz zawierający tekst, elektronika, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. **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.

1. **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](https://ipinfo.io/173.66.146.112)

1. **Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?**

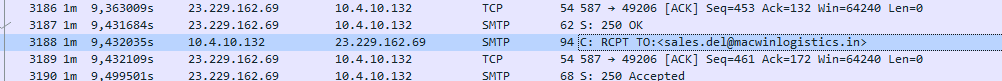
Przy pierwszej odpowiedzi w protokole SMTP – Simple Mail Transfer Protocol, możemy w szczegółach przeczytać informacje o oprogramowaniu.

Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

1. **To which email account is the stolen information sent?**

sales.del@macwinlogistics.in



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

Szukamy logowania:  
Obraz zawierający tekst, Czcionka, linia, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Możemy zdekodować wartość za pomocą Base64

Sales@23

1. **Which malware variant exfiltrated the data?**

Follow > TCP stream.

Mamy wartości maila:

Obraz zawierający tekst, zrzut ekranu, dokument, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Zakodowane w base64

Po zdekodowaniu nagłówek:  
HawkEye Keylogger - Reborn v9

Passwords Logs

1. **What are the bankofamerica access credentials? (username:password)**

Po zdekodowaniu możemy wyszukać bankofamerica (ctrl+f)

roman.mcguire:P@ssw0rd$

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