

Analisi di Rete

Sommario

| | |
|---|---|
| Traccia esercizio principale | 2 |
| Traccia esercizio facoltativo | 5 |
| Svolgimento esercizio principale | 6 |
| Analisi del Traffico..... | 6 |
| Scansione delle Porte | 6 |
| Identificazione delle Porte Aperte e Chiuse | 6 |
| Richieste ARP | 6 |
| Conclusioni | 6 |
| Svolgimento esercizio facoltativo | 7 |
| Cos'è il CSIRT Italia (ACN)..... | 7 |
| Compiti del CSIRT Italia..... | 7 |
| Analisi allerta Trenitalia | 7 |
| Come Proteggere l'Organizzazione | 7 |
| Cos'è il 4-Way Handshake..... | 8 |
| Fasi del 4-Way Handshake | 8 |
| Importanza del 4-Way Handshake..... | 8 |
| Report su Agent Tesla | 9 |
| Caratteristiche e Funzionalità | 9 |
| Dettagli Tecnici..... | 9 |
| Processo di Esecuzione..... | 9 |
| Incidenti e Diffusione..... | 9 |
| Conclusione | 9 |

Traccia esercizio principale

Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco



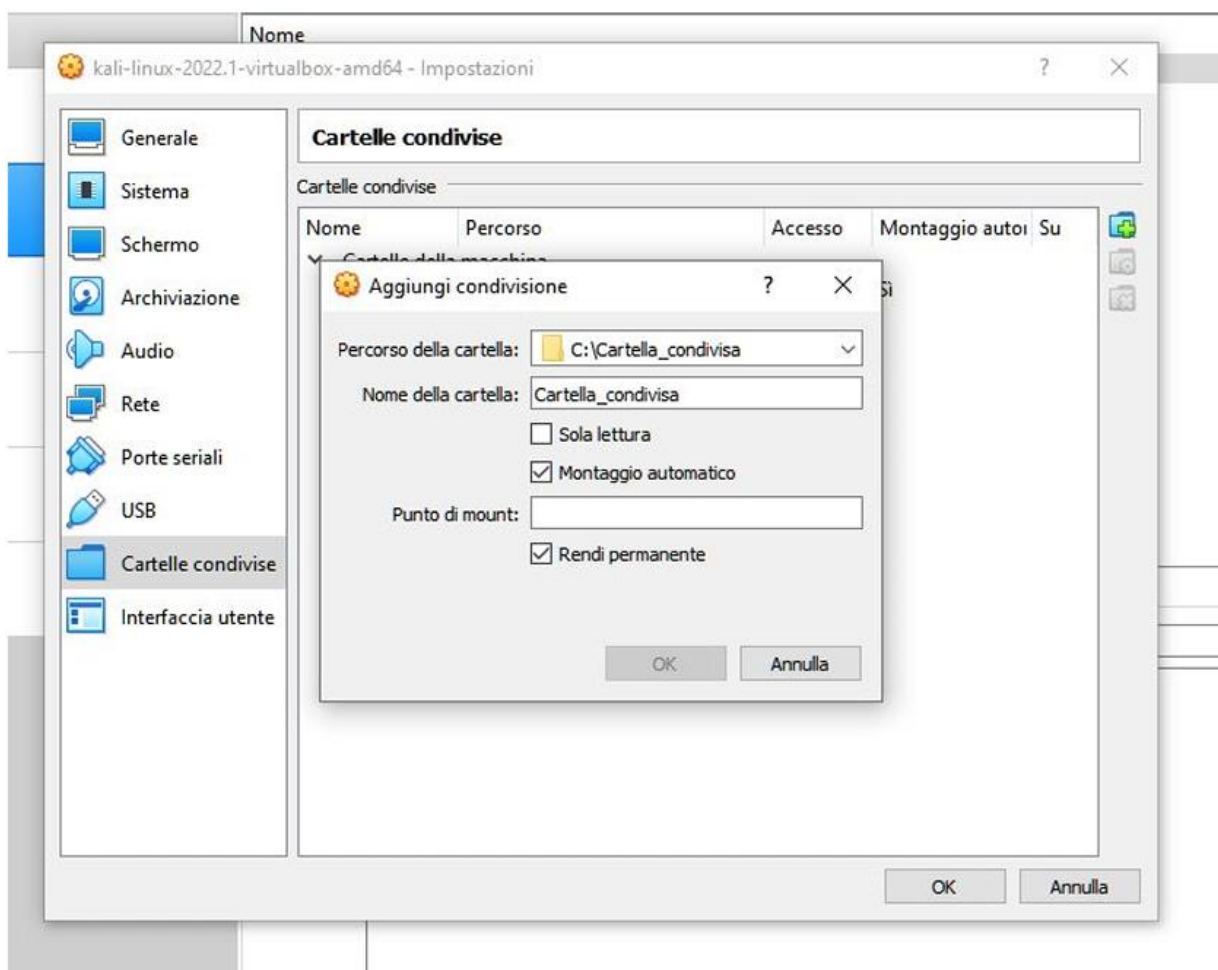
Cattura_U3_W1_L3.pcapng

Per analizzare la cattura, spostate il file sulla vostra Kali Linux, e fate doppio-click, vi aprirà la cattura direttamente con Wireshark, dopo aver configurato i permessi per l'utente Kali.

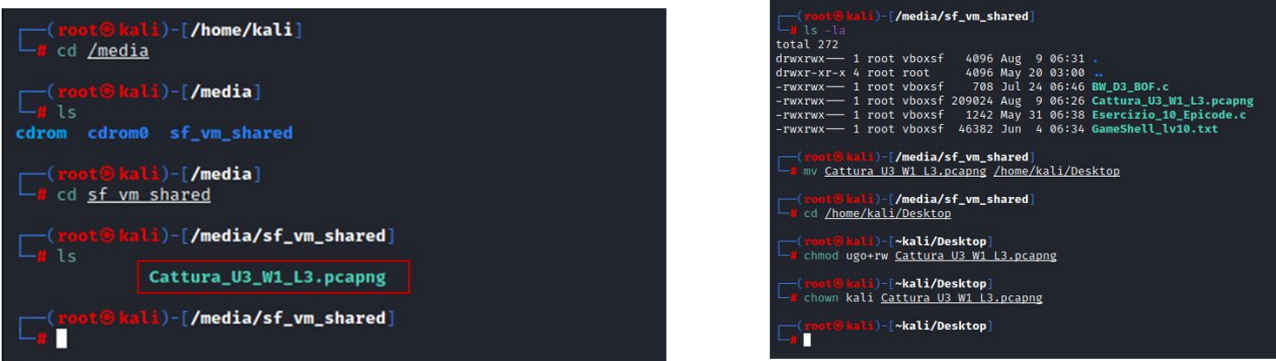
Potete spostare il file sulla vostra Kali creando una cartella condivisa tra il vostro host e la Kali come la figura a destra.

Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella.

Configurate la cartella con le opzioni in figura.



Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory /media come da figura seguente. Come vedete il nostro file è nella cartella condivisa. Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux (il comando che abbiamo usato noi è nella figura a destra). Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari - riferimento figura in a destra. A questo punto fate doppio click per analizzare la cattura.



Qualora doveste avere problemi per spostare il file su Kali, trovate una prima parte della cattura negli screenshot di seguito, sufficienti per completare l'esercizio.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------------|---------------------|-----------|--------|---|
| 1 | 0.00000000 | 192.168.200.150 | 192.168.200.255 | BROADCAST | 286 | Host Announcement: METASPLOITABLE, Workstation, Server, Print Queue Server, Xerox Server, NT Workstation, NT Server, Potential... |
| 2 | 23.764214995 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53860 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128 |
| 3 | 23.764215003 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 13307 - 33070 [RST] Seq=1 Ack=1 Win=0 Len=0 |
| 4 | 23.764777323 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 80 - 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427 WS=64 |
| 5 | 23.764777327 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 443 - 33070 [RST] Seq=1 Ack=1 Win=0 Len=0 |
| 6 | 23.764811329 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 53860 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 7 | 23.764899091 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 53860 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165 |
| 8 | 28.751629851 | PcsCompu...fd:87:1e | PcsCompu...39:7d:7e | ARP | 60 | Who has 192.168.200.100? Tell 192.168.200.150 |
| 9 | 28.751644519 | PcsCompu...39:7d:7e | PcsCompu...fd:87:1e | ARP | 42 | 192.168.200.100 is at 08:00:27:39:7d:7e |
| 10 | 28.774852257 | PcsCompu...39:7d:7e | PcsCompu...fd:87:1e | ARP | 42 | Who has 192.168.200.150? Tell 192.168.200.100 |
| 11 | 28.775238999 | PcsCompu...39:7d:7e | PcsCompu...fd:87:1e | ARP | 60 | 192.168.200.150 is at 08:00:27:fd:87:1e |
| 12 | 36.774143445 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41384 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128 |
| 13 | 36.774218116 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128 |
| 14 | 36.774257041 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33870 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128 |
| 15 | 36.774366395 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 58636 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 16 | 36.774405027 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52358 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 17 | 36.774535334 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46138 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 18 | 36.774614770 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 19 | 36.774658055 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 20 | 36.774658052 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 4111 - 54120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64 |
| 21 | 36.774658998 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 443 - 33070 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 22 | 36.774697327 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 551 - 580 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 23 | 36.774697376 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 24 | 36.774708464 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 41384 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 25 | 36.774711072 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466 |
| 26 | 36.775141104 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 27 | 36.775141273 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 21 - 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535438 WS=64 |
| 28 | 36.775174048 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 29 | 36.775373880 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 59174 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128 |
| 30 | 36.775486094 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 31 | 36.775524204 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53902 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 32 | 36.775589890 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 33 | 36.775619454 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 41384 - 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 34 | 36.775624907 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 54120 - 993 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 35 | 36.775799338 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 22 - 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=4294952466 |
| 36 | 36.775797084 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 37 | 36.775903786 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 38 | 36.775913232 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 53862 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 39 | 36.775920051 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 135 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 40 | 36.775975876 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 40 | 36.775975876 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 41 | 36.77605853 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 53862 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466 |
| 42 | 36.776179338 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 58634 - 159 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 43 | 36.776233880 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54220 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128 |
| 44 | 36.776336610 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 45 | 36.776385694 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33842 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 46 | 36.776420508 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45814 - 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 47 | 36.776451824 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 159 - 54094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 48 | 36.776451357 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 49 | 36.776478201 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 50 | 36.776496366 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33266 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 51 | 36.776512221 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 52 | 36.776568686 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49554 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 53 | 36.776671271 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37282 - 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 54 | 36.776720715 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54898 - 508 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 55 | 36.776813123 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 507 - 34040 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 56 | 36.776814342 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51531 - 497 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 57 | 36.776904828 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 445 - 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 58 | 36.776904922 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 59 | 36.776949461 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 139 - 46990 [RST, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 60 | 36.776950504 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 143 - 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 61 | 36.776950543 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 25 - 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 62 | 36.776950582 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 118 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 63 | 36.77695123 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64 |
| 64 | 36.776951592 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 509 - 24098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 65 | 36.776951772 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 53942 - 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 66 | 36.776954020 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 46990 - 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 67 | 36.776962328 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 60632 - 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 68 | 36.776963978 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466 |
| 69 | 36.777118401 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 457 - 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 70 | 36.777143614 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 56990 - 787 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 71 | 36.777186821 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35638 - 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128 |
| 72 | 36.777362991 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34120 - 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 73 | 36.777378354 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49780 - 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 74 | 36.777438632 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 787 - 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 75 | 36.777439741 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 436 - 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 76 | 36.777473818 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36138 - 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 77 | 36.777522494 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52420 - 982 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128 |
| 78 | 36.777623862 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 98 - 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 79 | 36.777623149 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 78 - 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 78 | 36.777623149 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 79 | 36.777645527 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41874 → 754 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535441 TSecr=0 WS=128 |
| 81 | 36.777680898 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51508 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535441 TSecr=0 WS=128 |
| 82 | 36.777758636 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 83 | 36.777758696 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 84 | 36.777871245 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 764 → 48174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 85 | 36.777871293 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 86 | 36.777883298 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 33842 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 TSecr=4294952460 |
| 87 | 36.777912717 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 46998 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 TSecr=4294952460 |
| 88 | 36.777886795 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 68632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 TSecr=4294952460 |
| 89 | 36.778831265 | 192.168.200.100 | 192.168.200.150 | TCP | 66 | 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535441 TSecr=4294952460 |
| 90 | 36.778179578 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535441 TSecr=0 WS=128 |
| 91 | 36.778200161 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 48448 → 896 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535441 TSecr=0 WS=128 |
| 92 | 36.778307839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55642 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 93 | 36.778305546 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 143 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 94 | 36.778385948 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 886 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 95 | 36.778449494 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 96 | 36.778482791 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42420 → 1807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 97 | 36.778591226 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 34846 → 286 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 98 | 36.778614095 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 99 | 36.778663864 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 100 | 36.778721880 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 286 → 34846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 101 | 36.778780327 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45810 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 102 | 36.778781327 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 103 | 36.778826294 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 104 | 36.778864493 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 105 | 36.778939322 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 52 → 45810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 106 | 36.778939427 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 107 | 36.778983153 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 108 | 36.779029210 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 109 | 36.779055543 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55642 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 110 | 36.779122229 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 111 | 36.779145084 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535442 TSecr=0 WS=128 |
| 112 | 36.779252884 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 887 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 113 | 36.779273761 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 114 | 36.779309462 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46886 → 196 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 115 | 36.779354564 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 948 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 116 | 36.779378639 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 58204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 117 | 36.779387623 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 118 | 36.779605540 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 118 | 36.779605648 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 119 | 36.779605750 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 186 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 120 | 36.779605898 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 138 → 58204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 121 | 36.779605843 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 122 | 36.779635753 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 123 | 36.779776288 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 124 | 36.779806041 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 125 | 36.779911109 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 53130 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 126 | 36.779946174 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 48522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 127 | 36.780035851 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 793 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 128 | 36.780121127 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 129 | 36.780149473 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 51552 → 93 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 130 | 36.780170333 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 48822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535443 TSecr=0 WS=128 |
| 131 | 36.780215176 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 42 → 48522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 132 | 36.780301750 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 133 | 36.780325040 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51232 → 121 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 134 | 36.780346429 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 46848 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 135 | 36.780409818 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38568 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 136 | 36.780427899 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 36846 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 137 | 36.780472609 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 52420 → 52 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 138 | 36.780498987 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38822 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 139 | 36.780577888 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 266 → 48822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 140 | 36.780577981 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 141 | 36.780578626 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 226 → 48848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 142 | 36.780578704 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 739 → 38548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 143 | 36.780578119 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 144 | 36.780578158 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 145 | 36.780578198 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 317 → 38802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 146 | 36.780613767 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42446 → 263 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 147 | 36.780781625 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 51152 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 148 | 36.780805705 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 991 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 149 | 36.780824718 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 150 | 36.780903109 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 241 → 51152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 151 | 36.780905648 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 152 | 36.780958367 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49614 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 153 | 36.781007559 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 154 | 36.781118680 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 155 | 36.781118917 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 137 → 49614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 156 | 36.781138769 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 157 | 36.781159927 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 157 | 36.781159927 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535444 TSecr=0 WS=128 |
| 158 | 36.781255484 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 159 | 36.781255593 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 160 | 36.781321950 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55368 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 161 | 36.781356928 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45848 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 162 | 36.781429319 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 163 | 36.781484705 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 918 → 55368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 164 | 36.781484720 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 512 → 45848 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=4294952466 TSecr=810535445 WS=64 |
| 165 | 36.781512468 | 192.168.200.100 | 192.168.200.150 | TCP | 60 | 45848 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535445 TSecr=4294952466 |
| 166 | 36.781621871 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 167 | 36.781640611 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 168 | 36.781734418 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35988 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 169 | 36.781816291 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 170 | 36.781898957 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 45848 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsv=810535445 TSecr=4294952466 |
| 171 | 36.782069902 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 663 → 35808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 172 | 36.782128748 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 32818 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 173 | 36.782140866 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35988 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 174 | 36.782215991 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 38259 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 175 | 36.782248180 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535445 TSecr=0 WS=128 |
| 176 | 36.782396780 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 681 → 39210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 177 | 36.782396883 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 561 → 47690 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 178 | 36.782396930 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 179 | 36.782396978 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 180 | 36.782422713 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 181 | 36.782459487 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 182 | 36.782534412 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 183 | 36.782582077 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 184 | 36.782696036 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 185 | 36.782696055 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 186 | 36.782698713 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 187 | 36.782705350 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 39210 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 188 | 36.782854473 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 189 | 36.782887993 | 192.168.200.150 | 192.168.200.100 | TCP | 74 | 41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 190 | 36.783026182 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 50 → 59484 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 191 | 36.783042408 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42626 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 192 | 36.783084241 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59484 → 928 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535446 TSecr=0 WS=128 |
| 193 | 36.783329650 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 194 | 36.783329795 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 874 → 42626 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 195 | 36.783329836 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 928 → 59110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 196 | 36.783391839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 Tsv=810535447 TSecr=0 WS=128 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 193 | 36.783329658 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 144 → 41184 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 194 | 36.783329795 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 195 | 36.783329836 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 928 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 196 | 36.783391839 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128 |
| 197 | 36.783426736 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57372 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128 |
| 198 | 36.783551923 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 964 → 42699 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 199 | 36.783557992 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 333 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 200 | 36.785397588 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 52872 → 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 201 | 36.785443154 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37888 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 202 | 36.785551321 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59832 → 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 203 | 36.785624918 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 47472 → 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 204 | 36.785675817 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 205 | 36.785675893 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 888 → 37888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 206 | 36.785721042 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41984 → 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 207 | 36.785738953 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57854 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 208 | 36.785824656 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 939 → 58932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 209 | 36.785824723 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 210 | 36.785889968 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 57402 → 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 211 | 36.785943368 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33719 → 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 212 | 36.786209855 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 213 | 36.786209978 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 122 → 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 214 | 36.786210019 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 215 | 36.786210029 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 359 → 33719 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 216 | 36.786254145 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 35164 → 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128 |
| 217 | 36.786292426 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59734 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 218 | 36.786455822 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 586 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 219 | 36.786455920 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 220 | 36.786708804 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45116 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 221 | 36.786815129 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 222 | 36.786864504 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 223 | 36.786899954 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 37052 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 224 | 36.787023089 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 545 → 45116 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 225 | 36.787023195 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 226 | 36.787069390 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 43106 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 227 | 36.787191086 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 239 → 38180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 228 | 36.787191781 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 520 → 37052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 229 | 36.787229817 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 42460 → 489 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128 |
| 230 | 36.787386591 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 769 → 43106 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 231 | 36.787346317 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 49988 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128 |
| 232 | 36.787470054 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 44644 → 846 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128 |

Traccia esercizio facoltativo

- Cos'è il CSIRT Italia ACN ?
- Quali sono i suoi compiti?
- Esamina l'allerta:
 - <https://www.csirt.gov.it/contenuti/campagna-phishing-a-tema-sondaggio-trenitalia-al03-240322-csirt-ita>
- Come puoi proteggere la tua organizzazione da questa campagna phishing?

Svolgimento esercizio principale

Questo report analizza il traffico di rete registrato tra i dispositivi 192.168.200.100 e 192.168.200.150, basato sui dati forniti nel file di Wireshark. Si ipotizza che il dispositivo target sia una macchina Metasploitable2, comunemente utilizzata come obiettivo per test di penetrazione.

Analisi del Traffico

Scansione delle Porte

L'attaccante ha probabilmente avviato una scansione delle porte. Le righe del file di Wireshark mostrano numerosi pacchetti TCP SYN inviati da 192.168.200.100 verso 192.168.200.150. Questa attività è tipica di una scansione stealth, come quella eseguita con Nmap utilizzando il flag -sS, che invia solo pacchetti SYN senza completare il three-way handshake.

Identificazione delle Porte Aperte e Chiuse

Le risposte RST ricevute dal dispositivo 192.168.200.150 (ad esempio, righe 5, 21, 26, e 47) indicano che molte delle porte tentate sono chiuse. Questo comportamento suggerisce che l'attaccante sta mappando le porte per identificare quali servizi sono attivi e quali potrebbero essere vulnerabili a exploit.

Richieste ARP

Le richieste ARP (righe 8-11) mostrano che i dispositivi stanno cercando di risolvere gli indirizzi IP associati ai propri indirizzi MAC. Questo è un passo necessario per la comunicazione nella rete locale e indica che il traffico è attivo.

Conclusioni

In sintesi, l'analisi del traffico, come evidenziato nel file di Wireshark, suggerisce che l'attaccante ha utilizzato una scansione delle porte per identificare il dispositivo Metasploitable2 come potenziale vittima. La scansione delle porte, probabilmente eseguita con Nmap utilizzando il flag -sS, ha rivelato porte chiuse tramite risposte RST.

Svolgimento esercizio facoltativo

Cos'è il CSIRT Italia (ACN)

Il **CSIRT Italia** è il team nazionale che si occupa della risposta agli incidenti informatici. Fa parte dell'Agenzia per la Cybersicurezza Nazionale (ACN) e ha il compito di supportare enti pubblici, aziende e cittadini nella gestione delle minacce informatiche.

Compiti del CSIRT Italia

I principali compiti del CSIRT Italia sono:

- **Monitoraggio:** Raccogliere e analizzare dati su minacce e vulnerabilità.
- **Risposta a Incidenti:** Offrire supporto tecnico in caso di attacchi informatici.
- **Prevenzione:** Sviluppare strategie per evitare attacchi.
- **Sensibilizzazione:** Informare e formare i cittadini e le aziende sulla sicurezza informatica.
- **Collaborazione:** Lavorare insieme ad altre agenzie internazionali e nazionali.

Analisi allerta Trenitalia

L'allerta riguardante una campagna di phishing a tema "sondaggio Trenitalia" avvisa gli utenti su email fraudolente che sembrano provenire da Trenitalia. Queste email invitano a partecipare a sondaggi e mirano a rubare informazioni personali.

Come Proteggere l'Organizzazione

Per difendersi da questa campagna di phishing, le organizzazioni possono adottare le seguenti misure:

1. **Formazione dei Dipendenti:** Educare i collaboratori a riconoscere email sospette.
2. **Filtri Antispam:** Utilizzare soluzioni per bloccare email pericolose.
3. **Verifica delle Comunicazioni:** Controllare sempre l'autenticità di email e link.
4. **Autenticazione a Due Fattori:** Implementare sistemi di sicurezza aggiuntivi per gli accessi.
5. **Aggiornamenti di Sicurezza:** Tenere software e sistemi operativi sempre aggiornati.
6. **Backup dei Dati:** Eseguire backup regolari per proteggere le informazioni aziendali.
7. **Segnalazione di Email Sospette:** Creare un protocollo interno per segnalare email o incidenti sospetti.

Adottando queste misure, le organizzazioni possono migliorare la loro sicurezza e ridurre il rischio di attacchi di phishing.

Cos'è il 4-Way Handshake

Il **4-Way Handshake** è un processo di autenticazione utilizzato nei protocolli di rete, in particolare nel protocollo Wi-Fi (802.11), per garantire una connessione sicura tra un client (come un computer o uno smartphone) e un punto di accesso (access point). Questo processo è fondamentale per stabilire una connessione sicura e per proteggere i dati trasmessi.

Fasi del 4-Way Handshake

Il 4-Way Handshake si compone di quattro passaggi principali:

1. Message 1: Il Client Richiede una Connessione

- Il client invia un messaggio al punto di accesso per iniziare la connessione. Questo messaggio contiene un identificatore unico (nonce) generato dal client.

2. Message 2: Il Punto di Accesso Risponde

- Il punto di accesso riceve il messaggio e risponde con un proprio nonce, insieme a una chiave di sessione che è derivata dalla chiave pre-condivisa (la password) e dai nonce scambiati. Questo messaggio è crittografato.

3. Message 3: Il Client Conferma la Connessione

- Il client riceve il secondo messaggio e utilizza le informazioni per generare la chiave di sessione. Poi invia un messaggio di conferma al punto di accesso, indicando che ha ricevuto correttamente il nonce e la chiave.

4. Message 4: Il Punto di Accesso Conferma la Connessione

- Infine, il punto di accesso invia un messaggio di conferma al client, completando il processo di autenticazione. A questo punto, entrambi i dispositivi possono iniziare a comunicare in modo sicuro utilizzando la chiave di sessione condivisa.

Importanza del 4-Way Handshake

- **Sicurezza:** Il 4-Way Handshake aiuta a prevenire attacchi come il "replay attack" e garantisce che solo i dispositivi autorizzati possano connettersi alla rete.
- **Crittografia:** Stabilisce una chiave di sessione che viene utilizzata per crittografare i dati trasmessi tra il client e il punto di accesso.
- **Autenticazione:** Verifica che entrambi i lati (client e punto di accesso) possano fidarsi l'uno dell'altro prima di iniziare a scambiare dati sensibili.

In sintesi, il 4-Way Handshake è un componente essenziale per garantire la sicurezza delle connessioni Wi-Fi.

Report su Agent Tesla

Agent Tesla è un tipo di malware, specificamente un **trojan di accesso remoto (RAT)**, scritto in **.NET**. È attivo dal 2014 e si concentra su sistemi operativi **Microsoft Windows**. Questo malware è molto versatile e ha diverse funzioni, tra cui il furto di informazioni sensibili, la registrazione di tasti e la cattura di schermate.

Caratteristiche e Funzionalità

Agent Tesla ha una serie di funzioni che lo rendono pericoloso:

1. **Furto di Credenziali:** Può raccogliere password, nomi utente, informazioni finanziarie e cronologia di navigazione da più di 50 applicazioni, come client di posta elettronica e browser web.
2. **Cattura di Schermate:** È in grado di fare screenshot del computer della vittima, raccogliendo informazioni sensibili.
3. **Intercettazione di Comunicazioni:** Può monitorare email, messaggi di chat e altre forme di comunicazione online.
4. **Registrazione di Tasti:** Monitora i tasti premuti, registrando informazioni sensibili come password e nomi utente.
5. **Caricamento e Download di File:** Può trasferire file dal computer della vittima e installare moduli aggiuntivi.
6. **Diffusione a Altri Sistemi:** Può propagarsi ad altri computer sulla rete sfruttando vulnerabilità.

Dettagli Tecnici

Agent Tesla utilizza tecniche di offuscamento, come l'encoding Base64 e la crittografia XOR, per nascondere il proprio codice e rendere più difficile il rilevamento da parte dei software di sicurezza. Inoltre, ha meccanismi anti-analisi per evitare di essere scoperto.

Processo di Esecuzione

La maggior parte delle campagne di Agent Tesla avviene in più fasi:

1. **Consegna:** Il malware viene inviato come allegato a un'email di spam, spesso in forma di documento di Office o file zip.
2. **Esecuzione:** Una volta aperto l'allegato, viene eseguito un downloader che scarica la seconda fase del malware.
3. **Raccolta delle Informazioni:** Il malware raccoglie informazioni dal sistema della vittima e le invia all'attaccante.

Agent Tesla utilizza diversi protocolli di comunicazione per inviare dati al server di comando e controllo, come **HTTP**, **SMTP**, **FTP** e **Telegram**.

Incidenti e Diffusione

Agent Tesla è stato utilizzato in molti attacchi informatici nel corso degli anni. Ha visto un aumento significativo durante la pandemia di COVID-19, con campagne che sfruttavano temi legati alla salute per ingannare le vittime. Ad esempio, nel 2020 sono state segnalate campagne che distribuivano Agent Tesla attraverso falsi aggiornamenti per dispositivi di protezione personale.

Nel 2022, è stato identificato come uno dei malware più diffusi nel settore educativo, colpendo circa il 7% delle organizzazioni a livello globale.

Conclusione

Agent Tesla è un malware pericoloso e versatile che continua a rappresentare una minaccia significativa per utenti e organizzazioni. La sua capacità di rubare informazioni sensibili e di diffondersi attraverso email di phishing sottolinea l'importanza di pratiche di sicurezza informatica rigorose, come la formazione degli utenti e l'uso di software di sicurezza aggiornati.

Fonti: https://en.wikipedia.org/wiki/Agent_Tesla