



THREAT INTELLIGENCE & IOC

NICHOL GALESSIERE

29/11/2024



COS'È LA THREAT INTELLIGENCE

La Threat Intelligence (Intelligence sulle minacce) è l'insieme di informazioni strategiche, tattiche e operative che vengono raccolte, analizzate e condivise per migliorare la comprensione delle minacce informatiche e rafforzare la difesa di un'organizzazione contro attacchi cibernetici. In pratica, la Threat Intelligence fornisce un quadro delle minacce potenziali o in corso e aiuta le organizzazioni a prepararsi, rispondere e mitigare i rischi derivanti da tali minacce.



IOC

IOC è l'acronimo di Indicators of Compromise (Indicatori di compromissione). Si tratta di elementi o dati che indicano che un sistema informatico è stato compromesso da un attacco o che un attacco informatico è in corso o è già avvenuto. Gli IOC possono essere utilizzati per rilevare, analizzare e rispondere a incidenti di sicurezza.



OBIETTIVI

Abbiamo analizzato un file di cattura del traffico di rete utilizzando Wireshark, un potente strumento per il monitoraggio della rete.

Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati

Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

ANALISI DEL TRAFFICO TCP

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	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 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	50684 → 199 [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	36.776330610	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	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [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	33206 → 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	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 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 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [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 → 33042 [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	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	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	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	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	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	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	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990 → 707 [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	36.777302991	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	36.777337934	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	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 580 [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	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623082	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

IOC E I POSSIBILI SCENARI

L'immagine precedente ci mostra un'analisi di pacchetti di rete.

Ecco quali potrebbero essere i potenziali indicatori di compromissione (IOC):

- Pacchetti TCP con troppi stati SYN e pochi stati ACK possono suggerire tentativi di scansione e ricerca di vulnerabilità
- Un numero elevato di pacchetti in un intervallo di tempo ridotto può segnalare attività malevola
- Potrebbe trattarsi di una comunicazione legittima tra dispositivi. Ad esempio, un client potrebbe accedere a un server per richiedere dati o servizi
- Molti pacchetti SYN potrebbero essere inviati per saturare le risorse del server, rendendolo non disponibile per gli utenti legittimi (Ddos).
- Porta di destinazione: Le porte di destinazione variano continuamente, tra porte note e porte dinamiche, non andando a colpire quindi una porta e un servizio specifico.
- Indirizzi IP coinvolti: IP sorgente (attaccante): 192.168.200.100 - IP destinazione (vittima): 192.168.200.150 Entrambi gli indirizzi sono locali, indicando che si tratta di un'unica rete interna.
- Oltre all'indirizzo IP privato, abbiamo la doppia conferma che l'attaccante è all'interno della rete in quanto il protocollo ARP agisce tra il livello 2 e il livello 3 del modello ISO/OSI e associa IP e indirizzi Mac, che vengono utilizzati solamente all'interno della rete locale. Non sono presenti tracce di ARP poisoning.

VETTORI DI ATTACCO



La scansione effettuata dall'attaccante potrebbe essere considerata sospetta, dato che precede la fase di attacco.

La scansione di porte in sé potrebbe non compromettere direttamente il sistema, ma espone i servizi disponibili al rischio di exploit. Se l'attaccante riesce a identificare una porta aperta su un servizio vulnerabile, può poi eseguire exploit specifici per prendere il controllo del sistema.

Nel traffico di rete, abbiamo osservato numerosi pacchetti SYN che, se inviati ripetutamente in un breve lasso di tempo, possono esaurire le risorse del server o dei dispositivi di rete, causando un SYN Flood, che è un tipo di attacco DoS.

L'attaccante potrebbe aver utilizzato una scansione come "nmap -sT -p-" che sfrutta interamente il three-way handshake previsto dal protocollo TCP.

Basandoci sugli IOC rilevati, l'attacco osservato potrebbe non considerarsi un vero e proprio attacco, bensì una scansione non stealth mirata sul dispositivo vittima

AZIONI DI MITIGAZIONE

per proteggere una rete e prevenire attacchi ecco quali potrebbero essere alcune azioni consigliate:

- configurare un firewall per bloccare traffico non autorizzato e non necessario e implementare regole di filtraggio specifiche per limitare l'accesso sulle porte
- mantenere tutti i software e i sistemi operativi aggiornati con le ultime patch di sicurezza impostando aggiornamenti automatici quando è possibile
- implementare un IDS/IPS per monitorare e rispondere ad attività sospette in tempo reale
- monitorare costantemente il traffico di rete per identificare comportamenti anomali
- eseguire backup regolari dei dati critici e verificare la possibilità di ripristino in caso di attacco
- eseguire regolari penetration testing per identificare e risolvere eventuali vulnerabilità
- formazione e sensibilizzare il personale sull' uso improprio degli strumenti di rete, spiegando le possibili conseguenze di attività come scansioni o altre attività di rete non autorizzate.