



Cybersecurity

Threat Intelligence & IOC

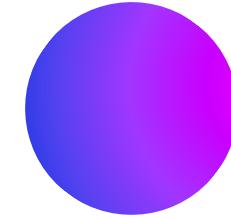
Di Carmine Malangone

Threat Intelligence

La Threat Intelligence consiste nel raccogliere dati da diverse fonti (interne o esterne), trasformarli in informazioni utili e contestualizzarli per fornire una comprensione chiara delle minacce. Questo aiuta i team di sicurezza a prendere decisioni informate per proteggere la rete, i sistemi e i dati aziendali.

La Threat Intelligence è fondamentale per proteggere le organizzazioni dalle minacce informatiche moderne. Non si limita a fornire dati, ma li trasforma in informazioni utilizzabili per anticipare, identificare e mitigare gli attacchi. La sua efficacia dipende dalla capacità di integrare queste informazioni nei processi di sicurezza aziendali e di mantenere un ciclo continuo di apprendimento e adattamento.

IOC (Indicator of Compromise)



Gli IOC sono strumenti essenziali per la sicurezza informatica. Consentono di rilevare, analizzare e prevenire gli attacchi informatici. La Threat Intelligence, sfruttando gli IOC, fornisce alle organizzazioni una visione più chiara del panorama delle minacce e le aiuta a prendere decisioni informate per proteggere i propri sistemi e dati.

Come vengono utilizzati gli IOC nella Threat Intelligence:

- **Rilevamento precoce:** Gli IOC consentono di rilevare tempestivamente un attacco in corso, prima che possa causare danni significativi.
- **Analisi forense:** Aiutano a ricostruire la cronologia di un attacco e a identificare le tecniche utilizzate dagli attaccanti.
- **Correlazione di minacce:** Consentono di collegare diversi incidenti e di identificare campagne di attacco più ampie.
- **Creazione di regole di sicurezza:** Gli IOC possono essere utilizzati per creare regole di firewall, sistemi di rilevamento delle intrusioni e altri controlli di sicurezza per prevenire futuri attacchi.
- **Condivisione di informazioni:** Gli IOC vengono condivisi tra organizzazioni e agenzie governative per migliorare la consapevolezza delle minacce e accelerare la risposta agli incidenti.



Definiamo gli Obiettivi

04

Approfondire gli argomenti.

01

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

02

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

03

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

Introduzione

Analizzando il file possiamo vedere che è stato inviato un gran numero di pacchetti SYN al ip 192.168.200.100 e possiamo ipotizzare che si tratti di:

- Un attacco Dos.
- Una scansione della rete aggressiva.

Nelle prossime slide approfondiremo come lo abbiamo capito e come ci si può difendere.



Cattura_U3_W1_L3.pcapng

Situazione

Come si può notare l'IP

192.168.200.150 invia pacchetti al IP **192.168.200.100**. La prima

cosa che notiamo è che i due dispositivi **sono sulla stessa rete**, questo ci fa capire che l'attacco sta avvenendo dal interno. Come si nota i pacchetti inviati non

concludono la stretta di mani a 3 vie inviando molti pacchetti SYN. Nelle prossime slide analizzeremo le possibili cause.

Source	Destination	Protocol	Length Info
2876 192.168.200.100	192.168.200.150	TCP	60 95656 - 22 [SYN, ACK] Seq=1 Ack=1 Win=4240 Len=0 Tsvcl=810532429 Tsecr=4294952466
2877 192.168.200.100	192.168.200.150	TCP	60 95653 - 80 [SYN, ACK] Seq=1 Ack=1 Win=4240 Len=0 Tsvcl=810532430 Tsecr=4294952466
3032 192.168.200.100	192.168.200.150	TCP	74 50684 - 197 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532430 Tsecr=0 WS=128
3888 192.168.200.100	192.168.200.150	TCP	74 54220 - 995 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532430 Tsecr=0 WS=128
3889 192.168.200.100	192.168.200.150	TCP	74 54648 - 587 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532430 Tsecr=0 WS=128
3890 192.168.200.100	192.168.200.150	TCP	74 54649 - 587 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532430 Tsecr=0 WS=128
3891 192.168.200.100	192.168.200.150	TCP	74 54650 - 587 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532430 Tsecr=0 WS=128
1284 192.168.200.150	192.168.200.100	TCP	60 139 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1357 192.168.200.150	192.168.200.100	TCP	60 995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8201 192.168.200.100	192.168.200.150	TCP	74 46980 - 139 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
8202 192.168.200.100	192.168.200.150	TCP	74 46981 - 139 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
2221 192.168.200.100	192.168.200.150	TCP	74 69532 - 25 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
8506 192.168.200.100	192.168.200.150	TCP	74 49554 - 119 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
1271 192.168.200.100	192.168.200.150	TCP	74 37282 - 53 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
1272 192.168.200.100	192.168.200.150	TCP	74 37283 - 53 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
1127 192.168.200.150	192.168.200.100	TCP	60 587 - 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3423 192.168.200.100	192.168.200.150	TCP	74 51534 - 487 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=128
4828 192.168.200.100	192.168.200.150	TCP	74 445 - 33042 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810532440 Tsecr=0 WS=64
4922 192.168.200.100	192.168.200.150	TCP	60 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4923 192.168.200.100	192.168.200.150	TCP	60 256 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5084 192.168.200.150	192.168.200.100	TCP	60 143 - 33296 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6043 192.168.200.150	192.168.200.100	TCP	74 245 - 66532 [SYN, ACK] Seq=0 Ack=0 Win=7532 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=4294952466 Tsecr=810535440 WS=64
5082 192.168.200.150	192.168.200.100	TCP	60 110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1273 192.168.200.150	192.168.200.100	TCP	74 37281 - 32265 [SYN, ACK] Seq=0 Ack=0 Win=0 Len=0
1467 192.168.200.150	192.168.200.100	TCP	60 209 - 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4772 192.168.200.100	192.168.200.150	TCP	66 33842 - 445 [ACK] Seq=0 Ack=1 Win=0 Len=0 Tsvcl=810535440 Tsecr=4294952466
1029 192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535440 Tsecr=4294952466
2329 192.168.200.100	192.168.200.150	TCP	66 69632 - 25 [ACK] Seq=1 Ack=1 Win=4256 Len=0 Tsvcl=810535440 Tsecr=4294952466
3717 192.168.200.100	192.168.200.150	TCP	66 72880 - 100 [ACK] Seq=1 Ack=1 Win=4256 Len=0 Tsvcl=810535440 Tsecr=4294952466
1481 192.168.200.150	192.168.200.100	TCP	60 487 - 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8014 192.168.200.100	192.168.200.150	TCP	74 56590 - 787 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535440 Tsecr=0 WS=128
6821 192.168.200.100	192.168.200.150	TCP	74 53538 - 436 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535440 Tsecr=0 WS=128
2991 192.168.200.100	192.168.200.150	TCP	74 34210 - 98 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535440 Tsecr=0 WS=128
2992 192.168.200.100	192.168.200.150	TCP	74 34211 - 98 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535440 Tsecr=0 WS=128
6537 192.168.200.100	192.168.200.150	TCP	60 787 - 56998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7741 192.168.200.100	192.168.200.150	TCP	60 436 - 35538 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3018 192.168.200.100	192.168.200.150	TCP	74 36318 - 589 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
2884 192.168.200.100	192.168.200.150	TCP	74 52428 - 962 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
3082 192.168.200.100	192.168.200.150	TCP	60 98 - 34128 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1144 192.168.200.100	192.168.200.150	TCP	74 521 - 35700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length Info
89 36. 777321149	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 49760 - 49760 [SYN, ACK] Seq=1 Ack=1 Win=0 Len=0
89 36. 777345027	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 41574 - 764 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
89 36. 777360898	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 51546 - 435 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
89 36. 777375806	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 962 - 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89 36. 777377586	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 963 - 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36. 777781349	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36. 777781349	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 765 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86 36. 777781349	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 766 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
87 36. 777781377	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 767 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
88 36. 777781377	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 768 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
89 36. 777803345	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 769 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36. 778179779	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 53459 - 148 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
92 36. 778307036	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 54560 - 221 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
93 36. 778305546	192.168.200.100	192.168.200.150	192.168.200.100	TCP	60 148 - 51456 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94 36. 778305546	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 42428 - 1087 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
95 36. 778305546	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 42429 - 1087 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=810535441 Tsecr=0 WS=128
96 36. 778305546	192.168.200.100	192.168.200.150	192.168.200.100	TCP	74 42430 - 1087 [SYN] Seq=0 Win=4240 Len=0 MSS=1400 SACK_PERM=1 Tsvcl=81053

IP attaccante

192.168.200.150

Possiamo vedere che questo è l'indirizzo del attaccante dato che da questo indirizzo partono molte richieste verso 192.168.200.100

IP vittima

192.168.200.100

Possiamo vedere che questo indirizzo riceve le richieste e cerca di bloccarle.

Port scanning

È visibile una sequenza di connessioni verso porte diverse dello stesso host. Questo è tipico di tecniche di scansione delle porte utilizzate per identificare i servizi attivi su una macchina.

Cos'è

Immagina di voler sapere se un server web è raggiungibile. Utilizzando uno strumento di port scanning, puoi inviare un pacchetto alla porta 80 (la porta standard per il servizio HTTP). Se il server è attivo e il servizio HTTP è in ascolto, riceverai una risposta.

Reset (RST)

È presente una grande quantità di pacchetti TCP con flag RST. Questo potrebbe indicare un tentativo di interrompere o manipolare connessioni esistenti, oppure un comportamento anomalo nella gestione delle connessioni TCP.

Cos'è ?

Quando un dispositivo invia un pacchetto TCP con il flag RST settato, sta essenzialmente dicendo all'altro dispositivo: "Interrompi immediatamente questa connessione, c'è un problema".

Tentativi ripetuti di handshake (SYN e ACK)

Si notano numerosi pacchetti con flag SYN seguiti da RST, indicando un possibile attacco di tipo SYN flood.

Questo tipo di attacco mira a sovraccaricare le risorse del sistema vittima, interrompendo il normale funzionamento

Cos'è

Immagina di voler avviare una conversazione telefonica: prima di iniziare a parlare, devi stabilire una connessione con l'altra persona. In modo simile, i dispositivi di rete utilizzano SYN e ACK per "stringersi la mano" prima di scambiare dati.

SYN flood

Nel traffico analizzato, si osservano:

- Molti pacchetti TCP con il flag SYN inviati al server.
- Assenza del pacchetto ACK necessario per completare l'handshake.
- Numerosi pacchetti RST (Reset) indicano che le connessioni vengono interrotte bruscamente, probabilmente a causa del sovraccarico.
- **Scopo:** L'attacco mira a saturare le risorse del server, impedendo l'accesso ai servizi da parte degli utenti legittimi.

Cos'è

Un attacco SYN flood è una tecnica utilizzata per rendere un server o un dispositivo di rete temporaneamente inutilizzabile, sovraccaricandolo con un gran numero di richieste di connessione incomplete. È una forma di Denial of Service (**DoS**) che sfrutta il meccanismo di handshake TCP.

Vettori d'attacco

Scansione di rete:

La connessione multipla verso porte differenti è indicativa di un attacco di ricognizione. Un attaccante potrebbe utilizzare questa tecnica per mappare i servizi attivi su un host e determinare eventuali vulnerabilità.

Cos'è

Una scansione di rete è un processo che permette di identificare i dispositivi connessi a una rete, i servizi attivi e le eventuali vulnerabilità presenti. Questo viene fatto inviando pacchetti di rete a diversi indirizzi IP e porte, analizzando poi le risposte.

Vettori d'attacco

Mitigazione

Isolare dispositivi compromessi

Identificare e isolare i dispositivi nella rete che potrebbero essere compromessi.

Bloccare gli indirizzi IP sospetti

Gli indirizzi IP che generano traffico sospetto possono essere bloccati.

Monitoraggio in tempo reale

Attivare il monitoraggio continuo del traffico di rete per rilevare ulteriori tentativi di attacco

Misure preventive.



Bloccare gli indirizzi IP sospetti

Configurare regole di firewall per bloccare immediatamente il traffico proveniente dagli IP interni identificati come origine del traffico SYN anomalo.



Aggiornare i sistemi e il software

Assicurarsi che tutti i dispositivi della rete siano aggiornati con le ultime patch di sicurezza, riducendo la probabilità di sfruttamento di vulnerabilità note.



Installare un sistema IDS/IPS

Utilizzare strumenti come Snort o Suricata per identificare e rispondere automaticamente a comportamenti sospetti



Educare il personale

Formare gli utenti interni sull'importanza della sicurezza informatica, per ridurre il rischio di compromissioni interne tramite phishing o altri metodi.

Conclusione



Dall'analisi della cattura di rete, emerge che la macchina di destinazione è sotto attacco, con un traffico anomalo caratterizzato da un elevato numero di pacchetti TCP SYN inviati in rapida successione. Questi pacchetti sembrano avere come obiettivo uno o più servizi specifici della macchina vittima.

In particolare:

- I pacchetti SYN generano un numero significativo di connessioni parziali, lasciando il server in stato SYN_RECV, ovvero in attesa del completamento dell'handshake TCP.
- Non vi è una corrispondenza tra le richieste SYN e le risposte ACK che completano il handshake, il che indica che il client (in questo caso l'attaccante) non ha intenzione di stabilire connessioni autentiche.
- Il comportamento osservato non sembra casuale, ma deliberato, con lo scopo di saturare le risorse del server, impedendo a eventuali utenti legittimi di accedere ai servizi.