Aprile 2017

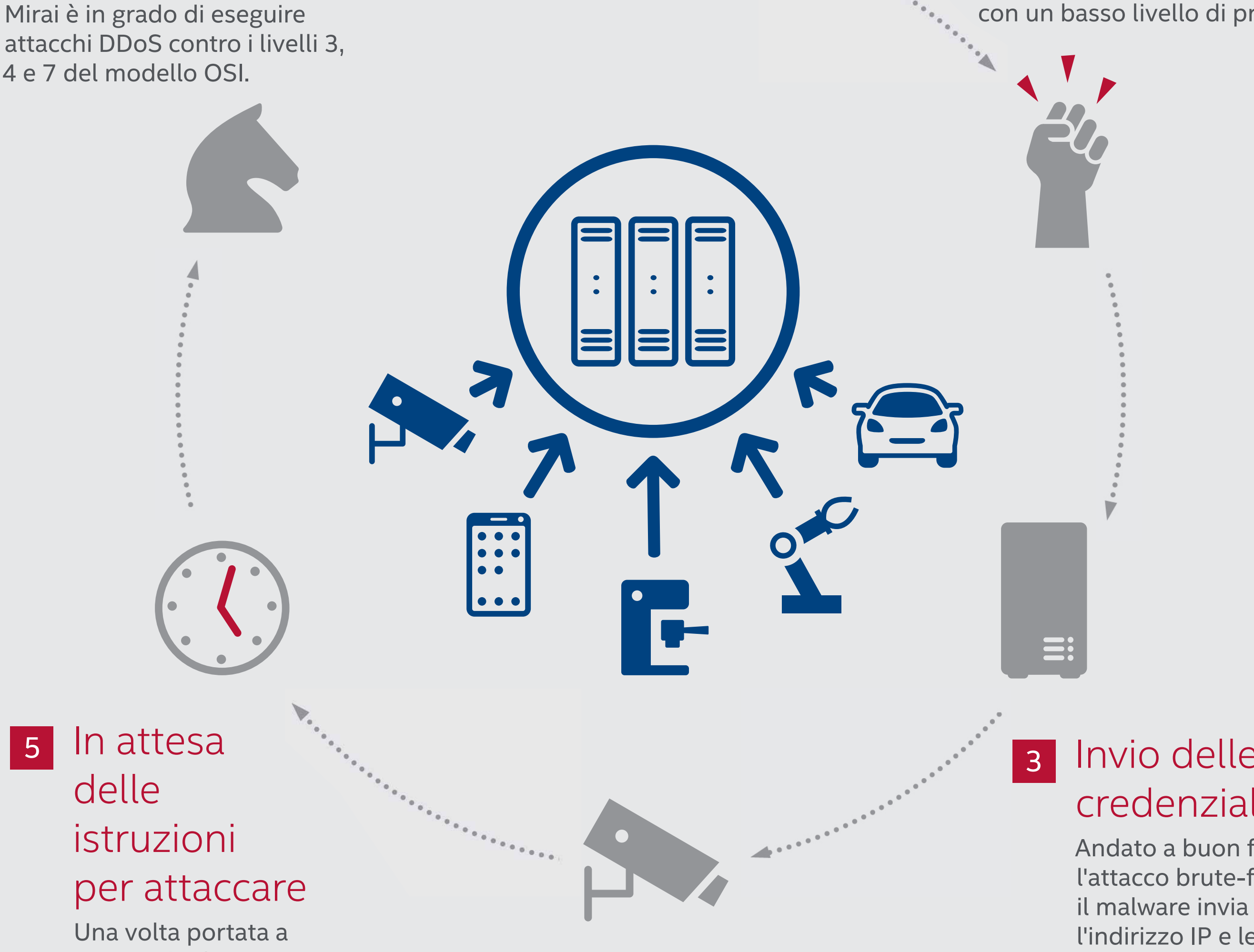
Report sulle minacce

McAfee Labs

Mirai, la botnet IoT

La botnet Mirai ha infettato e quindi sfruttato dispositivi IoT non adeguatamente protetti per eseguire l'attacco Denial-of-Dervice distribuito (DDoS) più esteso di sempre.

Il procedimento dell'attacco



1 Rilevamento dei dispositivi IoT

Mirai scansiona un'ampia gamma di indirizzi IP alla ricerca di porte Telnet o SSH aperte e individua i dispositivi IoT collegati.

2 Attacco brute-force

Mirai quindi lancia un attacco brute-force su tali dispositivi IoT utilizzando un dizionario di nomi utente e password di default comuni per identificare i dispositivi con un basso livello di protezione.

3 Invio delle credenziali

Andato a buon fine l'attacco brute-force, il malware invia l'indirizzo IP e le credenziali del dispositivo IoT compromesso al server di controllo.

4 Download del bot Mirai

Un server di carico scarica il codice binario del bot Mirai sul dispositivo IoT.

5 In attesa delle istruzioni per attaccare

Una volta portata a termine l'infezione, il malware sul dispositivo IoT rimane in attesa delle istruzioni per lanciare un attacco DDoS.

6 Avvio dell'attacco DDoS

Mirai è in grado di eseguire attacchi DDoS contro i livelli 3, 4 e 7 del modello OSI.

2,5 milioni

Mirai ha infettato circa 2,5 milioni di dispositivi IoT.

5 al minuto

Ogni minuto, circa cinque indirizzi IP vengono aggiunti alle botnet Mirai.

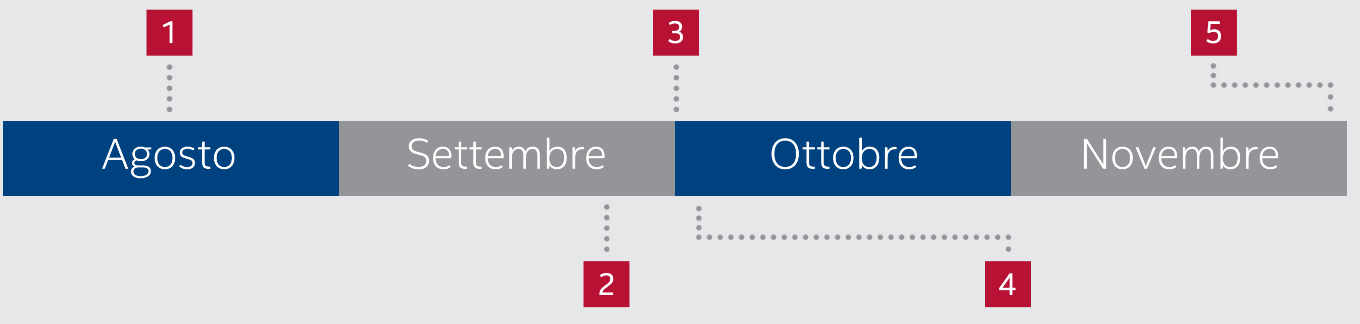
1,2 Tbps di traffico

Nel momento di picco, l'obiettivo di una botnet Mirai è stato inondato da 1,2 Tbps di traffico, il volume più elevato di traffico DDoS mai registrato.

da 50 a 7.500 dollari al giorno

Gli attacchi DDoS basati su Mirai vengono oggi offerti come un servizio con un costo variabile dai 50 ai 7.500 dollari al giorno.

Cronologia temporale dell'evoluzione di Mirai



1 *Intorno ad agosto 2016*
Rilascio iniziale di Mirai
I codici binari ELF di Mirai iniziano ad affiorare.

2 *20 settembre 2016*
Attacco DDoS al sito web "Krebs on Security"
Mirai infetta registratori DVR e TV a circuito chiuso sulla porta Telnet.

3 *sabato 1 ottobre 2016*
Rilascio del codice sorgente di Mirai
Anna-Senpai rilascia il codice sorgente di Mirai.

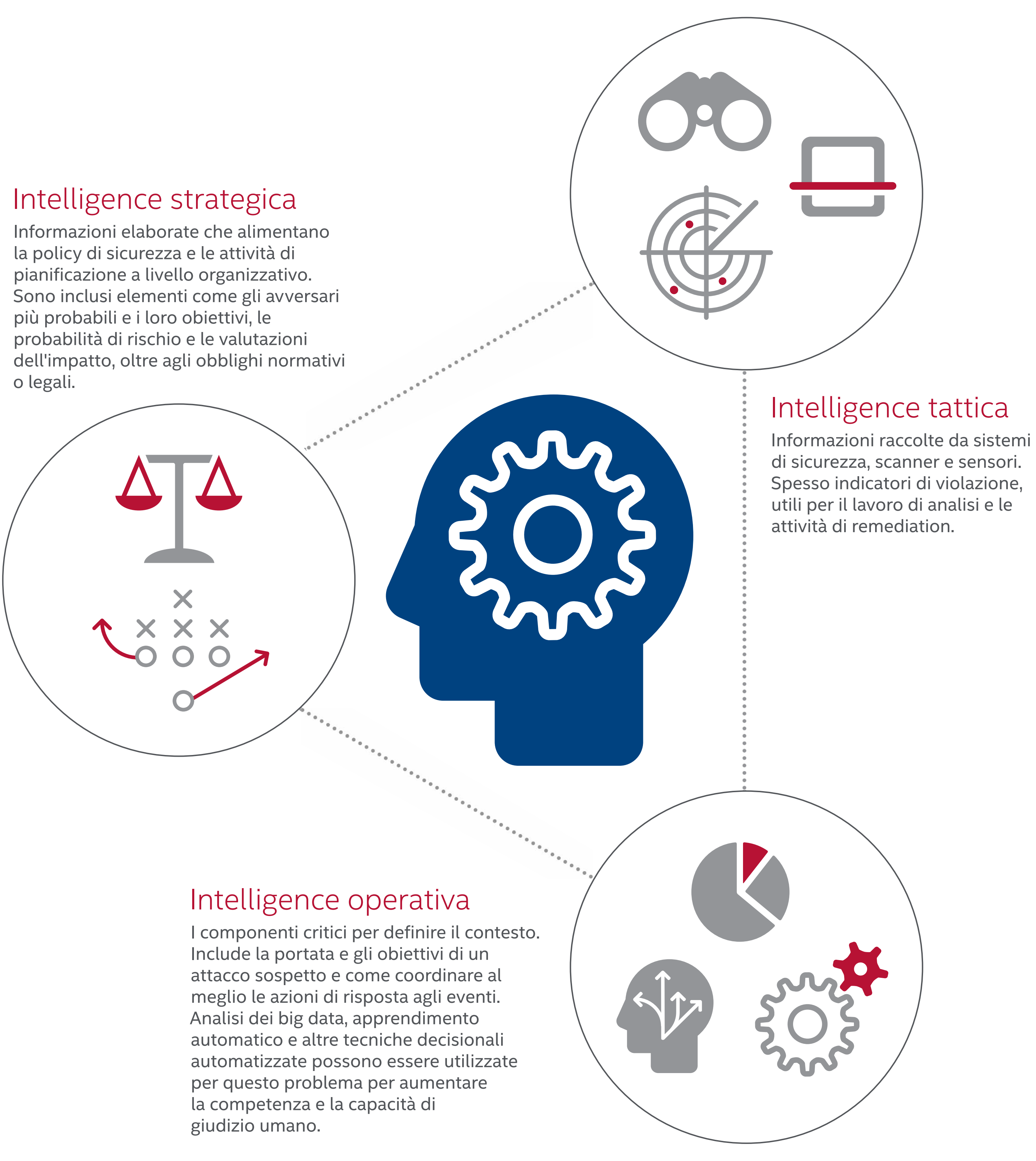
4 *4 ottobre 2016*
Mirai diventa una botnet-as-a-service
Un forum clandestino offre attacchi DDoS-as-a-service.

5 *28 novembre 2016*
Blackout di Deutsche Telekom
Individuata una nuova variante di Mirai. Prende di mira le porte 7547.

Condivisione dell'intelligence sulle minacce

Ciò che non conosci può ferirti.

Che cosa si intende con Threat Intelligence?



Intelligence strategica

Informazioni elaborate che alimentano la policy di sicurezza e le attività di pianificazione a livello organizzativo. Sono inclusi elementi come gli avversari più probabili e i loro obiettivi, le probabilità di rischio e le valutazioni dell'impatto, oltre agli obblighi normativi o legali.

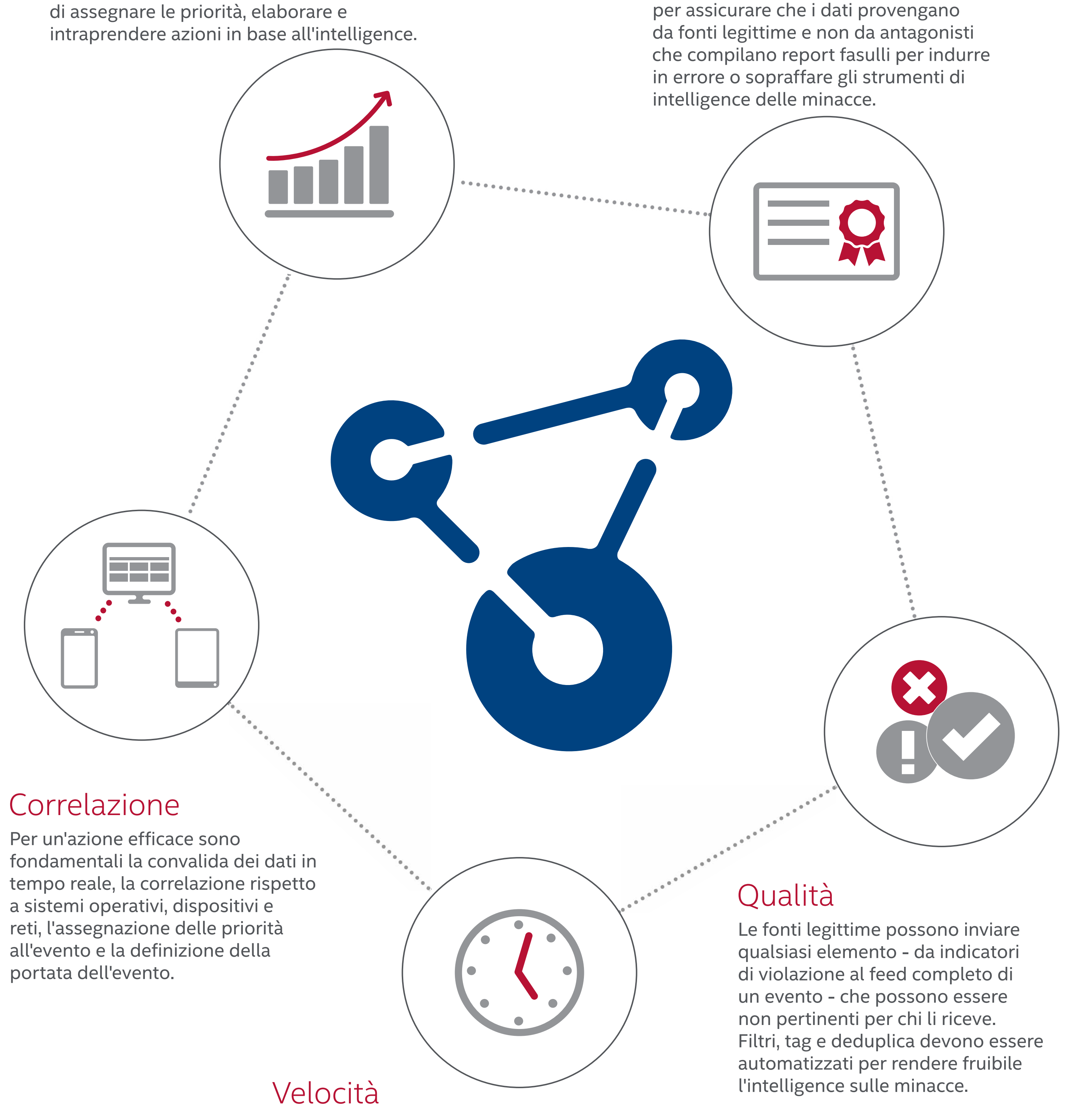
Intelligence tattica

Informazioni raccolte da sistemi di sicurezza, scanner e sensori. Spesso indicatori di violazione, utili per il lavoro di analisi e le attività di remediation.

Intelligence operativa

I componenti critici per definire il contesto. Include la portata e gli obiettivi di un attacco sospetto e come coordinare al meglio le azioni di risposta agli eventi. Analisi dei big data, apprendimento automatico e altre tecniche decisionali automatizzate possono essere utilizzate per questo problema per aumentare la competenza e la capacità di giudizio umano.

Le sfide critiche nella condivisione dell'intelligence sulle minacce



Volume

Sensori di sicurezza, analisi dei big data e strumenti di apprendimento automatico hanno creato un enorme problema di segnale-rumore che influenza la capacità di assegnare le priorità, elaborare e intraprendere azioni in base all'intelligence.

Convalida

È necessario esaminare le fonti dell'intelligence sulle minacce condivisa per assicurare che i dati provengano da fonti legittime e non da antagonisti che compilano report fasulli per indurre in errore o sopraffare gli strumenti di intelligence delle minacce.

Correlazione

Per un'azione efficace sono fondamentali la convalida dei dati in tempo reale, la correlazione rispetto a sistemi operativi, dispositivi e reti, l'assegnazione delle priorità all'evento e la definizione della portata dell'evento.

Velocità

Una comunicazione aperta, standardizzata e in tempo reale è fondamentale per limitare il ritardo tra il rilevamento di un attacco e la ricezione dell'intelligence sulle minacce.

Qualità

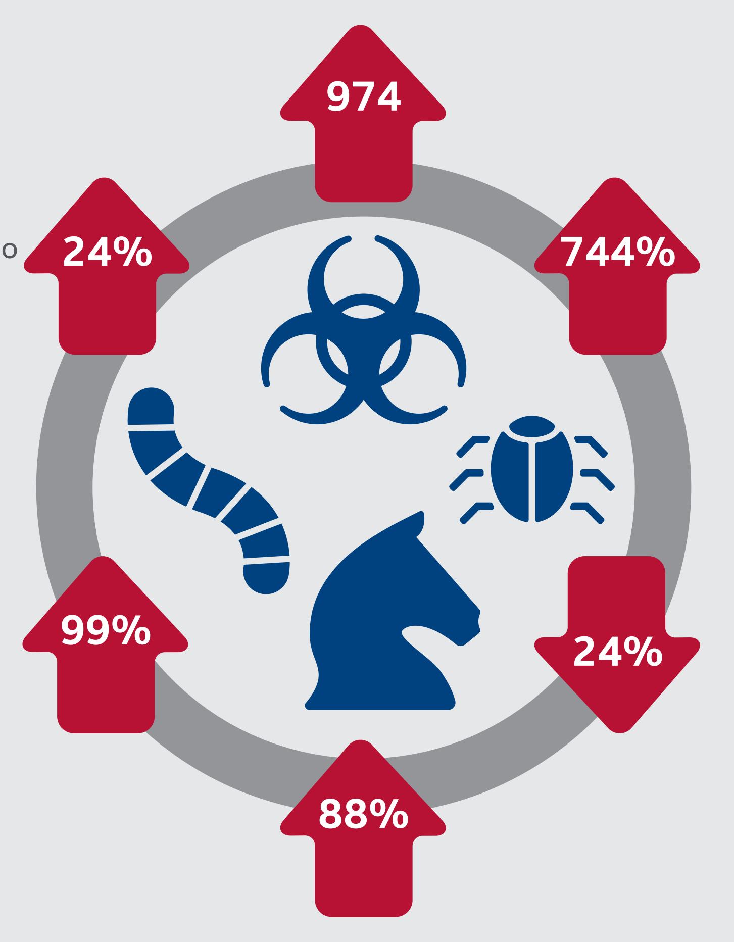
Le fonti legittime possono inviare qualsiasi elemento - da indicatori di violazione al feed completo di un evento - che possono essere non pertinenti per chi li riceve. Filtri, tag e deduplica devono essere automatizzati per rendere fruibile l'intelligence sulle minacce.

Statistiche sulle minacce

Emergono 176 nuove minacce ogni minuto, ovvero quasi 3 ogni secondo.

Incidenti

Abbiamo contato 197 incidenti pubblici noti nel quarto trimestre e 974 nel 2016.



Malware

Il numero di nuovi esempi di malware nel quarto trimestre - 23 milioni - è sceso del 17% rispetto al terzo trimestre. **Tuttavia, nel 2016 il conteggio complessivo è aumentato del 24% raggiungendo i 638 milioni di esempi.**

Malware mobile

Nel quarto trimestre il numero di nuovi esempi di malware mobile è diminuito del 17%. **Il malware mobile complessivo è invece aumentato del 99% nel 2016.**

Ransomware

Il numero di nuovi esempi di ransomware è sceso del 71% nel quarto trimestre, principalmente a causa del calo dei rilevamenti di ransomware generico e della diminuzione di Locky e CryptoWall. **Nel 2016, il numero complessivo di esempi di ransomware è aumentato dell'88%.**

Malware per il sistema operativo Mac

Anche se ancora contenuto rispetto alle minacce di Windows, il numero di nuovi esempi di malware per il sistema operativo Mac è cresciuto del 245% nel quarto trimestre, a causa del bundling con l'adware. **Il malware complessivo per il sistema operativo Mac è aumentato del 744% nel 2016.**

Botnet di spam

Le email di spam provenienti dalle 10 principali botnet è sceso del 24% nel quarto trimestre per un totale di 181 milioni di email. Queste 10 botnet hanno generato 934 milioni di messaggi email di spam nel 2016.

McAfee Global Threat Intelligence

McAfee GTI ha ricevuto in media 49,6 miliardi di interrogazioni al giorno.

McAfee GTI

66 milioni

Le protezioni di McAfee GTI dagli URL pericolosi sono **aumentate a 66 milioni al giorno nel quarto trimestre** dai 57 milioni al giorno del terzo trimestre.

37 milioni

Le protezioni di McAfee GTI contro i programmi indesiderati (PUP) sono **aumentate a 37 milioni al giorno nel quarto trimestre** dai 32 milioni al giorno del terzo trimestre.

71 milioni

Le protezioni di McAfee GTI dai file pericolosi sono **scese a 71 milioni al giorno nel quarto trimestre** dai 150 milioni al giorno del terzo trimestre, principalmente grazie a un maggior blocco dei download.

35 milioni

Le protezioni di McAfee GTI contro gli indirizzi IP pericolosi sono **aumentate a 35 milioni al giorno nel quarto trimestre** dai 27 milioni al giorno del terzo trimestre.

Report McAfee Labs sulle Minacce: aprile 2017

Visita www.mcafee.com/April2017ThreatsReport per il report completo.

intel Security

2614_0217_info-threat-report-mirai-iot