proofpoint

ET INTELLIGENCE

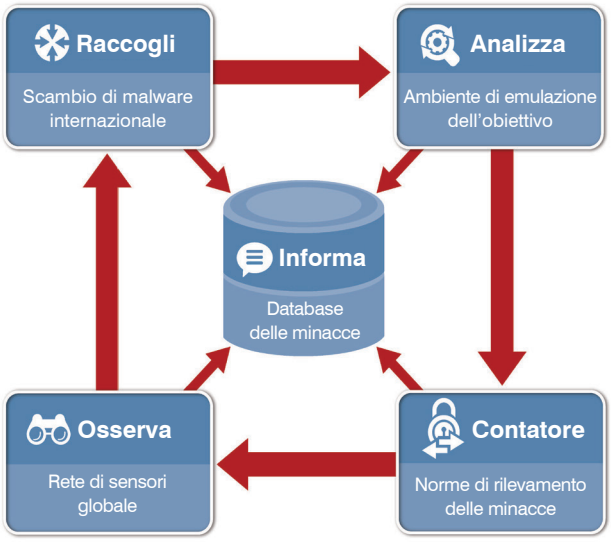
PUNTI SALIENTI

- Mantenete il passo con il panorama dinamico delle minacce grazie a dati di intelligence continuamente aggiornati.
- Bloccate gli attacchi e le campagne prima che raggiungano la vostra organizzazione.
- Aumentate il ritorno sull'investimento della vostra infrastruttura di sicurezza corrente grazie a semplici set di dati facili da utilizzare.
- Adottate una configurazione di sicurezza in base a dati di intelligence reali.
- Verificate che i vostri dispositivi di prevenzione operino secondo quanto pubblicizzato cercando gli indicatori di attività post-compromissione.
- Arricchite i dati di registro esistenti con una prospettiva globale su indirizzi IP e domini sospetti.
- Fate rispettare politiche di sicurezza personalizzate sulla base di categorie di reputazione e soglie di punteggio rilevanti per la vostra organizzazione.

Proofpoint ET Intelligence™ è la fonte di dati di intelligence sulle minacce più puntuale e precisa del settore. Unendo feed operativi IP e di reputazione del dominio aggiornati al minuto, e con un database di minacce osservate su scala globale e di analisi dei malware, ET Intelligence offre al professionista della sicurezza i dati di intelligence necessari per fermare prontamente gli attacchi dannosi e fornire il contesto necessario per le indagini.

PERCHÉ PROOFPOINT ET INTELLIGENCE?

Oggi, campagne di cyber attacchi vengono attuate con frequenza crescente da una varietà di attori, con motivazioni che vanno dai profitti allo spionaggio. Mentre gli strumenti di base impiegati per eseguire questi attacchi hanno degli elementi in comune e sono spesso derivati da meno di 20 kit di exploit conosciuti, ciascuna campagna risulta unica nel suo utilizzo di botnet, proxy, vettori di attacco e sistemi di controllo e comando. Data la natura dinamica di queste campagne, è diventato praticamente impossibile per le imprese mantenere il ritmo del panorama di attacco in costante cambiamento. Ed è lì che entra in gioco Proofpoint.



Il team di ricercatori specializzati negli attacchi e i sistemi analitici di Proofpoint ET Labs lavorano per sollevarvi da quest'onere. Il risultato è quello di avere dati di intelligence sulle minacce, originali al 100%, su indirizzi IP, domini, campioni di malware e kit di exploit ottenuti dall'osservazione diretta. Costruito su un processo proprietario che sfrutta uno dei più ampi siti di scambio di malware, l'emulazione della vittima su scala massiccia, una tecnologia di rilevamento originale e una rete globale di sensori, Proofpoint ET Intelligence viene aggiornato in tempo reale per fornire alle organizzazioni dati di intelligence operativi per combattere le minacce emergenti odierne.

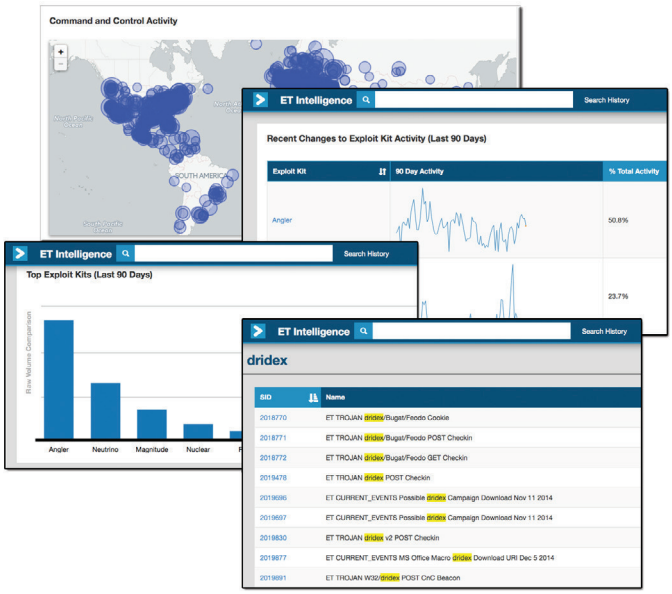
Proofpoint ET Intelligence, costituito dai feed di reputazione di indirizzi IP e domini, oltre che dal database globale delle minacce, offre sia dati di intelligence operativi sulle minacce sia una preziosa fonte di informazioni contestuali per agevolare le indagini sugli incidenti e la ricerca sulle minacce.

REPUTAZIONE IP E DOMINI DINAMICA

ET Intelligence fornisce feed di dati di intelligence operativi sulle minacce per l'inserimento su firewall, sistemi di rilevamento intrusioni/di protezione (IDS/IPS), sistemi di gestione e registrazione eventi (SIEM) e sistemi di autenticazione. Questi feed dinamici identificano gli IP e i domini coinvolti in attività sospette e dannose, come osservato direttamente da ET Labs di Proofpoint.

Le caratteristiche includono:

- Elenchi separati per indirizzi IP e domini.
- IP e domini classificati in oltre 40 categorie e catalogati con un punteggio di fiducia (da 0 a 127) per ciascuna categoria.
- Punteggi che indicano i recenti livelli di attività e riflettono l'invecchiamento aggressivo.
- Elenchi e punteggi aggiornati ogni ora e svalutati aggressivamente.
- Più formati, compresi TXT, CSV, JSON, e formati compressi.



Database globale delle minacce di Proofpoint ET Intelligence

DATABASE GLOBALE DELLE MINACCE

Le organizzazioni hanno imparato che non è abbastanza conoscere semplicemente i tipi di minacce esistenti, ma per prevenire gli attacchi e ridurre i rischi è necessario inoltre comprendere il contesto storico dell'origine di tali minacce, chi si cela dietro di esse, quando hanno attaccato, quali metodi hanno impiegato e perché. Proofpoint ET Intelligence offre agli utenti l'accesso on-demand ai metadati storici di IP, domini e ad altri dati di intelligence correlati relativi alle minacce, utili per assistere l'indagine e la ricerca sulle minacce.

Le caratteristiche includono:

- Accesso on-demand a dati di intelligence storici e correnti relativi alle minacce. Ricercabili per indirizzo IP, dominio, MD5 del malware, ID firma ET e messaggio testuale.
- I risultati di ricerca rivelano le informazioni correlate per le operazioni di pivot e drill down, fornendo una traccia dati utile ad accelerare le indagini sull'incidente.
- Oltre 5 anni di osservazione delle attività delle minacce.
- Dati aggiornati continuamente.
- Dashboard con panoramica della posizione globale corrente della minaccia su comandi e controlli e sui kit di exploit attivi.
- Disponibilità tramite l'interfaccia web dell'utente o tramite l'API

SICUREZZA STRATIFICATA PROOFPOINT

I singoli sistemi di sicurezza possono essere efficaci nel bloccare determinati tipi di minacce ma, senza una copertura completa, la compromissione è inevitabile.

- Ottenete dati di intelligence operativi in tempo reale e contesti globali utili al rilevamento di minacce avanzate con ET Intelligence.
- Indagate sugli attacchi basati su e-mail tramite Targeted Attack Protection e Proofpoint Enterprise Protection.
- Approfondite i dati forensi sulle minacce più avanzate segnalati dall'URL Defense Service e dall'Attachment Defense Service.
- Indagate sulle minacce bloccate da Threat Response.
- Utilizzate i dati di intelligence per estendere le capacità di difesa dei dati sensibili e riservati grazie a Proofpoint Enterprise Privacy.

MIGLIORAMENTO DEI DATI E DEGLI STRUMENTI ESISTENTI

L'infrastruttura odierna della sicurezza di rete include firewall, firewall di nuova generazione (NGFW), appliance di gestione unificata delle minacce (UTM), piattaforme di gestione degli eventi relativi agli incidenti di sicurezza (SIEM) e sistemi di autenticazione, fra gli altri. Ciascuno di questi elementi può essere reso più efficace con dati di intelligence puntuali relativi alle minacce.

Utilizzare i feed di reputazione per:

- Bloccare i collegamenti verso/da indirizzi IP a elevato rischio nei firewall, NGFW, IPS/IDS e UTM, aumentando l'efficacia di questi dispositivi.
- Sollevare obiezioni sugli indirizzi IP sospetti all'interno di sistemi di autenticazione basati sul rischio.
- Arricchire i dati di registrazione e degli eventi sulle piattaforme SIEM.
- Alimentare i sistemi analitici predittivi.
- Identificare le risorse compromesse e indagare sull'estensione delle infezioni interne.

Utilizzare il database globale delle minacce per:

- Investigare sugli incidenti.
- Collegare specifiche campagne di attacco a miliardi di indicatori individuali di compromissione.
- Cercare e visualizzare gli attacchi e gli attori in azione nel mondo.
- Fare ricerca sui malware, con panoramiche sul traffico di rete prodotto quando viene eseguito un campione di malware.
- Effettuare l'integrazione in SEIM per arricchire il contesto delle indagini.

CONTATTATE PROOFPOINT OGGI STESSO

Il panorama odierno delle minacce è un campo di battaglia impari, in cui i difensori devono proteggere più fronti, mentre gli attaccanti devono solo trovare una singola apertura. Le protezioni correnti, indipendentemente dalla complessità, potrebbero non essere sufficienti. Se applicati prontamente e se forniti di contesto, i dati operativi di intelligence possono fare la differenza fra una violazione di grave entità e un'intrusione marginale.

INFORMAZIONI SU PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), società di sicurezza informatica di nuova generazione, consente alle aziende di proteggere la modalità di lavoro odierna dei propri dipendenti dalle minacce avanzate e dai rischi di conformità. Proofpoint aiuta i professionisti della sicurezza informatica a proteggere i propri utenti dagli attacchi avanzati che li prendono di mira (tramite e-mail, app mobili e social media), a proteggere le informazioni importanti create dai dipendenti e a dotare i team dell'intelligenza e degli strumenti giusti per rispondere rapidamente quando insorgono problemi. Aziende leader di tutte le dimensioni, tra cui oltre il 50 per cento di quelle presenti in Fortune 100, si affidano alle soluzioni di Proofpoint, che sono create per gli ambienti IT odierni mobili e social e sfruttano sia la potenza del cloud sia una piattaforma di analisi basata su big data per combattere le moderne minacce avanzate.