

# PROTEZIONE DAGLI ATTACCHI MIRATI

## PROTEGGERE I DIPENDENTI DALLE MINACCE AVANZATE NELLE E-MAIL

Gli autori degli attacchi sfruttano gli strumenti utilizzati dalle persone per compromettere endpoint, rubare credenziali e accedere ai propri dati. Questo spiega perché oltre il 90% degli attacchi mirati continua a raggiungere le vittime mediante le e-mail.

Le soluzioni tradizionali di sicurezza informatica, che utilizzano tecniche obsolete quali reputazione e firme, non sono più sufficienti per identificare e bloccare le e-mail dannose. Le tecniche di malware si sono rapidamente evolute e, per restare al passo, deve fare altrettanto la tecnologia utilizzata per proteggere da tali minacce.

Targeted Attack Protection (TAP) di Proofpoint aiuta a rilevare, attenuare e bloccare le minacce avanzate che prendono di mira le persone attraverso le e-mail. Rileviamo attacchi noti e nuovi, mai visti prima, che utilizzano allegati e URL dannosi per installare malware su un dispositivo o per ingannare gli utenti inducendoli a condividere la password oppure altre informazioni sensibili. TAP è ineguagliabile nel blocco degli attacchi mirati che utilizzano malware polimorfici, documenti utilizzati come armi e phishing di credenziali per accedere a informazioni sensibili o rubare denaro.

**TAP fornisce la prima linea di difesa presso il gateway e-mail. TAP comprende due componenti:**

**Attachment Defense (Difesa allegati):** TAP può mantenere i messaggi finché non si riceve un verdetto a seguito dell'analisi dell'allegato. I messaggi puliti sono inviati alla casella di posta in arrivo, mentre le minacce sono poste in quarantena.

**URL Defense (Difesa URL):** messaggi che contengono URL riconosciuti come dannosi sono immediatamente messi in quarantena. TAP riscrive tutti gli altri URL per monitorare e bloccare i clic. Quando gli utenti fanno clic sugli URL riscritti, TAP li reindirizza, in base al verdetto dell'ispezione, alla pagina web originale o a una pagina di blocco personalizzabile che impedisce l'accesso al sito compromesso.

### BLOCCARE LE MINACCE PRIMA CHE RAGGIUNGANO LA CASELLA DI POSTA IN ARRIVO

TAP è costruito sulla piattaforma di sicurezza e-mail di Proofpoint di nuova generazione, che offre chiara visibilità di tutte le comunicazioni e-mail. Ciò implica che TAP dispone di maggiore contesto per estrarre intelligence delle minacce, per mitigare rapidamente la superficie dell'attacco bloccando i messaggi dannosi e per ridurre i rischi di sicurezza.

Altre soluzioni per minacce avanzate disponibili sul mercato possono esaminare il traffico SMTP via cavo per provare a rilevare le minacce sulla rete. In questo approccio manca il contesto per capire chi è colpito dalla minaccia e manca la capacità di ispezionare il traffico della rete

### VANTAGGI CHIAVE

- **Bloccare le minacce prima che raggiungano la casella di posta in arrivo**
- **Rilevare le minacce note e sconosciute nelle e-mail**
- **Rispondere con informazioni end-to-end**
- **Applicare rapidamente e proteggere totalmente**

crittografato. Pertanto, queste soluzioni dispongono solo di una visione limitata del panorama di minaccia delle e-mail. Analogamente, dal momento che non sono presenti nel flusso delle e-mail, non possono bloccare le minacce zero-day prima che raggiungano la casella di posta in arrivo delle persone.

### RILEVARE MINACCE NOTE E SCONOSCIUTE UTILIZZANDO TECNICHE ADATTABILI, SOFISTICATE

Il panorama delle minacce è in costante evoluzione. Ecco perché le nostre soluzioni di minacce avanzate si adattano costantemente alla rilevazione di nuovi modelli di attacco. TAP ispeziona l'intera catena di attacchi utilizzando tecniche statiche e dinamiche. Analizziamo le potenziali minacce in diverse fasi utilizzando approcci multipli per esaminare comportamento, codice e protocollo. Poiché la prevenzione è fondamentale, le nostre soluzioni sono progettate per rilevare le minacce nella catena degli attacchi appena possibile. TAP utilizza funzionalità esclusive, come ad esempio l'analisi predittiva, per identificare e nascondere gli URL sospetti prima che gli utenti possano farvi clic.

Riconosciamo che gli attacchi possono variare l'approccio al fine di evitare il rilevamento. Alcune minacce, come ad esempio il phishing di credenziali, non lasciano tracce evidenti. Le nostre tecnologie sono create non solo per rilevare le minacce ma anche per imparare da esse. Possiamo osservare modelli, tattiche, comportamenti e strumenti di ciascun attacco, rendendo il successivo più facile da rilevare.

## RISPONDERE CON INFORMAZIONI END-TO-END E INTELLIGENCE DI SICUREZZA SUPERIORE

Proofpoint rappresenta l'unica società di sicurezza informatica con intelligence delle minacce che copre e-mail, rete, app mobili e social media. Il nostro grafico delle minacce di intelligence basata sulla comunità contiene oltre 600 miliardi di punti dati per correlare le campagne di attacchi tra diversi settori e aree geografiche. Dal momento che possiamo attribuire la maggior parte del traffico dannoso alle campagne, si possono facilmente distinguere attacchi ad ampio spettro e minacce mirate a leadership dirigenziale o ad altri dipendenti di alto livello.

Integriamo le informazioni da Emerging Threats (ET) Intelligence di Proofpoint, la fonte più tempestiva e precisa di intelligence delle minacce sul mercato. L'ET Intelligence di Proofpoint rappresenta il gold standard per i ricercatori delle minacce, offrendo intelligence delle minacce verificata al 100% oltre a domini e indirizzi IP.

TAP di Proofpoint include una dashboard basata su web che fornisce i dati a livello organizzativo, di minaccia e di utente per aiutare ad assegnare priorità agli avvisi e agire. Sono fornite in tempo reale dettagliate informazioni di analisi forensi su minacce singole e campagne.

### Aiutiamo a rispondere a domande critiche, quali:

- Di che minaccia si tratta? Fa parte di una campagna di attacco?
- Chi è preso di mira?
- Quanti messaggi sono stati bloccati?
- Quali utenti hanno fatto clic?
- Come posso identificare se un endpoint è stato compromesso?

**GOOGLE DRIVE PHISHING - MARCH**  
103 Messages • 1329 Proofpoint Customers • 2 People Impacted

**Description**  
In Google Drive phishing, attackers attempt to steal a victim's Google account credentials through the use of a fake Google Drive login page. In the attack, the actor crafts a fake Google Drive login page and embeds the URL for this page in a phishing email. Some cases have been observed where the phishing page is itself hosted on a Google Drive, but in the majority of cases it is on a server controlled by the attacker.

**Attack Spread**  
150% WIDESPREAD  
Seen by 1329 Proofpoint Customers

**At Risk Users**  
No users are at risk for this threat

**Forensics**  
Delivery: Credential Phishing  
Malware: No data available  
Actor: TA300  
Reports: Report #10: 2016/03/02 04:13 UTC | Windows XP SP3

**Impacted Users**  
Users whose clicks were permitted to this threat

USER	CLICKS	LATEST CLICK
1332080c@university...	1	2016/03/24 13:19 UTC
b68f833@university...	1	2016/03/03 18:52 UTC

**Attack Progression**

MESSAGES	CAUGHT	DELIVERED	NOT REWRITTEN	BLOCKED	PERMITTED
103	83	20	0	0	2

**Threat Activity By Users**

All activity related to this threat seen in your organization's traffic:

- 5e45c72a@university-of-education.edu.zz
- 81168540@university-of-education.edu.zz
- 47100696@university-of-education.edu.zz

## APPLICAZIONE RAPIDA E PROTEZIONE TOTALE PER OTTENERE VALORE IMMEDIATO

Per proteggere i propri dipendenti, dati e marchi, le difese odierne devono agire nell'ambiente di lavoro del dipendente e al suo ritmo. L'architettura TAP consente rapida applicazione e immediato ricavo di valore. È possibile proteggere centinaia di migliaia di utenti non in settimane o mesi, ma solo in giorni.

La nostra soluzione protegge gli utenti su qualsiasi rete o dispositivo, indipendentemente da dove o come controllano le e-mail. TAP di Proofpoint viene facilmente configurato come modulo aggiuntivo alla piattaforma di sicurezza e-mail di Proofpoint, che può essere applicato come servizio cloud, dispositivo virtuale o hardware. Proofpoint utilizza inoltre il cloud per aggiornare istantaneamente il nostro software quotidianamente per incorporare rapidamente nuove funzionalità e aiutare ad anticipare gli attaccanti.

### 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.