proofpoint.

La verità dietro il social engineering

Basta luoghi comuni

Più conosci i tuoi dipendenti, le loro vulnerabilità, i loro privilegi e coloro che desiderano danneggiarli, meglio puoi contrastare gli attacchi di social engineering. Ma così come noi miglioriamo la nostra capacità di identificare le potenziali minacce, i criminali informatici adattano i loro metodi e si comportano in modi talvolta inaspettati.

Per aiutarti a tenere testa alle minacce, ti presentiamo le ultime tendenze, i comportamenti inediti e alcuni luoghi comuni sui criminali informatici e sui loro metodi di attacco.

Luogo comune N.1

I criminali informatici preferiscono gli attacchi lampo

La realtà:

I criminali informatici spesso dedicano tempo a fare ricerche e creare relazioni prima di sferrare un attacco.

TA453

Il gruppo TA453, al soldo del governo iraniano, utilizza spesso conversazioni innocue nelle sue campagne per estorcere informazioni alle vittime.

TA406

Il gruppo TA406 affiliato al regime nordcoreano cerca di acquisire le credenziali d'accesso delle vittime e altre informazioni prima di inviare link o allegati dannosi.

TA499

Il gruppo TA499, al soldo della Russia, ha inviato email apparentemente innocue per estorcere informazioni a personalità di spicco prima di lanciare i suoi attacchi.

Luogo comune N. 2

Servizi legittimi come quelli forniti da Google e Microsoft possono essere utilizzati in modo sicuro.

La realtà:

i criminali informatici sfruttano continuamente servizi legittimi per raccogliere credenziali d'accesso nonché ospitare e distribuire malware.

14%

Il 14% di tutte le campagne dannose osservate sfrutta servizi legittimi.

Gli URL che reindirizzano a Google sono quelli abusati più di frequente...

Ma gli URL che reindirizzano a Microsoft hanno ricevuto più del doppio di clic rispetto a quelli ospitati da Google.

Luogo comune N. 3

I criminali informatici utilizzano solo l'email

La realtà:

L'avanzato sistema di threat intelligence di Proofpoint ha identificato un numero crescente di attacchi che utilizzano email che menzionano un call center.

250.000

Proofpoint ha osservato oltre 250.000 attacchi tramite telefono (TOAD, Telephone-Oriented Attack Delivery) ogni giorno.

Le email TOAD non contengono link o allegati. Incoraggiano le vittime a chiamare un call center fasullo.

50.000 dollari

In un caso, una vittima ha perso quasi 50.000 dollari a seguito di un attacco TOAD.

Luogo comune N. 4

I thread delle conversazioni interne sono sicuri

La realtà:

L'hijacking del thread di discussione o delle conversazioni, è una tecnica diffusa tra molti criminali informatici molto attivi motivati dal guadagno.

x500

Proofpoint ha osservato oltre 500 campagne che sfruttano l'hijacking dei thread delle conservazioni

x16

... per distribuire 16 diverse famiglie di malware...

... tra cui Qbot, Emotet, IcedID e Racoon Stealer.

Luogo comune N.5

I criminali informatici utilizzano solo contenuti standardizzati a carattere professionale

La realtà:

I criminali informatici sfruttano gli eventi di tendenza, l'attualità, la cultura popolare e molto altro per incoraggiare le vittime a interagire con contenuti dannosi.

Ogni mese nel 2021, Proofpoint ha osservato centinaia di milioni di esche a tema COVID.

Le truffe legate al pagamento delle tasse sono tra le tecniche preferite dai criminali informatici, che offrono sconti in cambio di diverse informazioni sensibili.

Tra le altre esche osservate troviamo San Valentino Squid Game, il conflitto tra Ucraina e Russia e il supporto per i rifugiati.

Per saperne di più

Scarica il report Proofpoint sul social engineering

Risorse aggiuntive

LEGGI IL BLOG

Scopri le tattiche di social engineering più strane del 2021 in questo articolo del blog redatto dal team di ricercatori sulle minacce informatiche di Proofpoint.

ASCOLTA IL PODCAST

Social Engineering: come i criminali informatici manipolano i loro obiettivi. In questo podcast, Proofpoint spiega come i criminali informatici sfruttano il fattore umano per attaccarci.

ENTRIAMO IN CONTATTO →

Fissa un appuntamento con Proofpoint per scoprire come possiamo proteggere la tua azienda. Facci delle domande sulle nostre valutazioni gratuite dei rischi.

Per maggiori informazioni, visita il nostro sito all'indirizzo proofpoint.com/it

PROTEGGI I TUOI DIPENDENTI. DIFENDI I TUOI DATI.

I criminali informatici sanno che i tuoi utenti sono il modo più semplice per infiltrarsi nella tua azienda. Difendili. Proteggili. Dai loro i mezzi per proteggersi con Proofpoint. Ogni giorno proteggiamo i dipendenti di più aziende Fortune 500 e Global 2000 di qualsiasi altro fornitore del mercato.

Analizziamo...

Oltre 2,6 miliardi di email

Oltre 49 miliardi di URL

Oltre 1,9 miliardi di allegati

Oltre 28,2 milioni di account cloud

Oltre 1,7 miliardi di messaggi mobile

...ogni giorno.

proofpoint.