proofpoint

RAPPORTO

EMAIL FRAUD THREAT REPORT

ANALISI ANNUALE

RAPPORTO SULLE MINACCE DI FRODE VIA E-MAIL

proofpoint.com

La frode via e-mail, altrimenti nota come compromissione della corrispondenza digitale aziendale (BEC), rappresenta una delle principali minacce informatiche odierne. Questi attacchi socialmente progettati mirano agli individui piuttosto che alla tecnologia. Essi sono altamente mirati, vengono inviati in piccoli volumi e impersonano figure autoritarie.

La frode via e-mail fa leva sulla natura umana, ossia sulla paura, sulla ricerca di gratificazione e così via, per rubare denaro e informazioni preziose a dipendenti, clienti e partner commerciali.

Proofpoint ha analizzato più di 160 miliardi di e-mail inviate a oltre 2400 aziende in 150 Paesi.

Seguono i risultati relativi al 2017.

LA FRODE VIA E-MAIL CONTINUA A ESPANDERSI

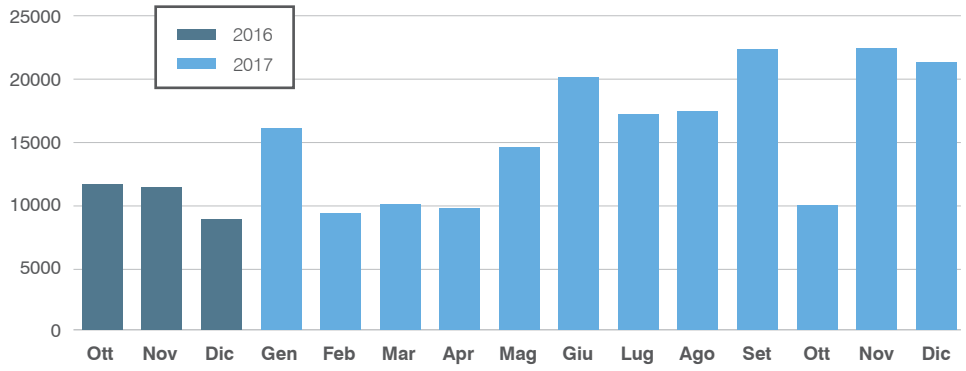
FRODE VIA E-MAIL
Gli attacchi fraudolenti via e-mail consistono nel richiedere al destinatario l'invio di un bonifico bancario o dei propri dati sensibili tramite un'e-mail o una serie di e-mail che fingono di provenire da un dirigente o da una ditta partner. Per essere ancora più difficili da rilevare e bloccare, non utilizzano allegati o URL dannosi.

LA FRODE VIA E-MAIL ha colpito il 2017 in modo dilagante. Se da una parte la minaccia continua a essere altamente mirata, gli attacchi sono stati lanciati contro un maggior numero di organizzazioni e più di frequente rispetto al 2016.

La percentuale di aziende colpite da almeno un attacco fraudolento via e-mail è salita con un ritmo costante, raggiungendo un nuovo picco dell'88,8% nel T4, ossia un aumento di 13,8 punti percentuali rispetto al 75,0% delle organizzazioni colpite nel trimestre dell'anno appena trascorso.

In media, le aziende sono state attaccate da 18,5 e-mail fraudolente per trimestre, registrando un aumento del 17% rispetto all'anno precedente. Tirando le somme, l'anno è terminato con due dei tre trimestri più colpiti da frodi via e-mail finora.

Attacchi basati sulla compromissione della corrispondenza digitale aziendale rilevati e bloccati da Proofpoint
Il T3 e il T4 sono stati due dei tre trimestri caratterizzati dal volume più elevato di frodi via e-mail finora.



I TRUFFATORI SI ADDENTRANO NEI MEANDRI DELLE ORGANIZZAZIONI

I criminali sono andati oltre lo spoofing di tipo "CEO-CFO", estendendo la propria portata all'interno delle organizzazioni.

Spoofing di più identità

Dopo aver mantenuto un ritmo costante per i primi tre trimestri, il numero medio di individui truffati per organizzazione è più che raddoppiato a circa 10 identità nel T4.

Alla base di questo cambiamento vi è una spiegazione valida. Mentre i team addetti alla sicurezza si sforzano sempre più di mettere in guardia i dipendenti contro le minacce di spoofing CEO, i malviventi trovano altre figure autoritarie da impersonare. Circa la metà (47%) delle organizzazioni ha dovuto assistere allo spoofing di oltre cinque identità nel T4, una cifra quasi raddoppiata rispetto all'intero trimestre precedente.

Più ruoli professionali nel mirino

La media complessiva degli individui colpiti all'interno di una data organizzazione si è stabilizzata a circa 13 individui nel T4. Tuttavia, i criminali prendono di mira sempre più figure professionali e sempre più gruppi aziendali all'interno di un'organizzazione, come per esempio le risorse umane (HR) e il reparto contabilità. In molti casi, essi riescono ad architettare un'e-mail convincente utilizzando tecniche di social engineering e le informazioni sui dipendenti ampiamente disponibili sul Web e sui social media.

Mentre gli aggressori cercavano di mietere sempre più vittime, il 41% delle aziende colpite nel T4 ha subìto attacchi che hanno truffato più di cinque identità e preso di mira più di cinque dipendenti.

ATTACCHI DI TIPO UNO-UNO

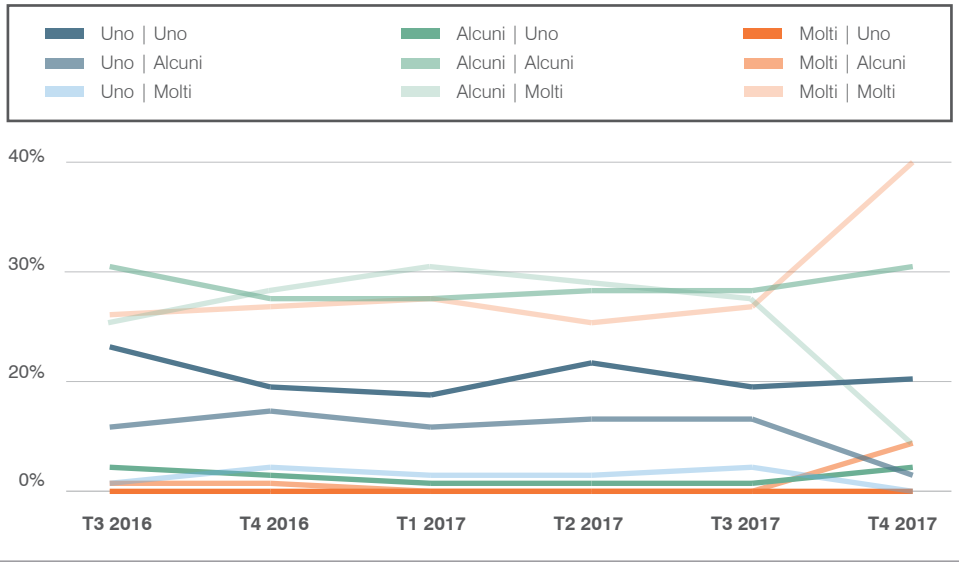
Nella frode via e-mail di tipo uno-uno, un truffatore assume un'identità (generalmente il CEO) e prende di mira un destinatario (di solito il CFO).

ATTACCHI DI TIPO MOLTI-MOLTI

Negli attacchi di tipo molti-molti, i truffatori impersonano più dirigenti e prendono di mira più destinatari. Per esempio, un truffatore potrebbe provare a impersonare più responsabili e prendere di mira l'intero team finanziario di un'azienda.

Identità falsificate VS e-mail inviate

Allontanandosi dai semplici attacchi di tipo **uno-uno**, i truffatori impersonano sempre più figure autoritarie e prendono di mira sempre più individui all'interno dell'organizzazione. Questi attacchi si definiscono attacchi di tipo **molti-molti**.



PER GLI AGGRESSORI, LE DIMENSIONI NON CONTANO

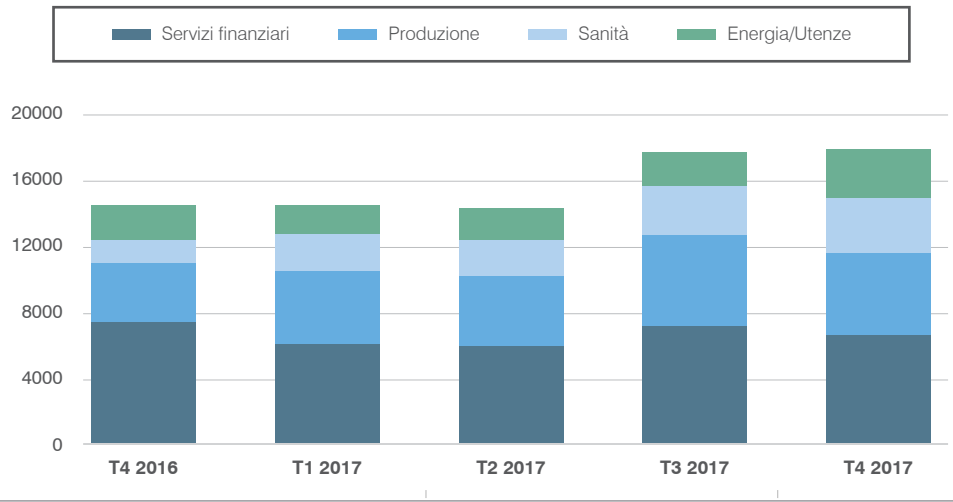
I truffatori colpiscono organizzazioni di qualsiasi dimensione. Inoltre, adottano un atteggiamento opportunistico in quanto prendono di mira qualsiasi settore.

Attacchi rivolti ad aziende di qualsiasi dimensione

Da quando abbiamo iniziato a raccogliere le informazioni sulle frodi nel 2016, abbiamo riscontrato una correlazione pressoché assente tra le dimensioni dell'azienda e la frequenza con cui quest'ultima riceve e-mail fraudolente. Tuttavia, c'è stato soltanto un trimestre (il T2 del 2017) che non ha mostrato la benché minima correlazione: gli aggressori hanno rivelato una lieve predisposizione verso prede più grandi.

Gli aggressori colpiscono molti settori

Il settore finanziario e il settore manifatturiero sono alcuni dei settori colpiti più di frequente. Tuttavia, abbiamo assistito ad attacchi fraudolenti via e-mail diffusi in tutti i settori.



La ricaduta degli attacchi su mire alte e basse in modo omogeneo potrebbe sembrare sorprendente. Ma, dal punto di vista degli aggressori, questo schema è più che giustificato. Infatti, se da una parte le organizzazioni più grandi sono probabilmente anche quelle più redditizie, le organizzazioni minori sono spesso più vulnerabili alle minacce avanzate.

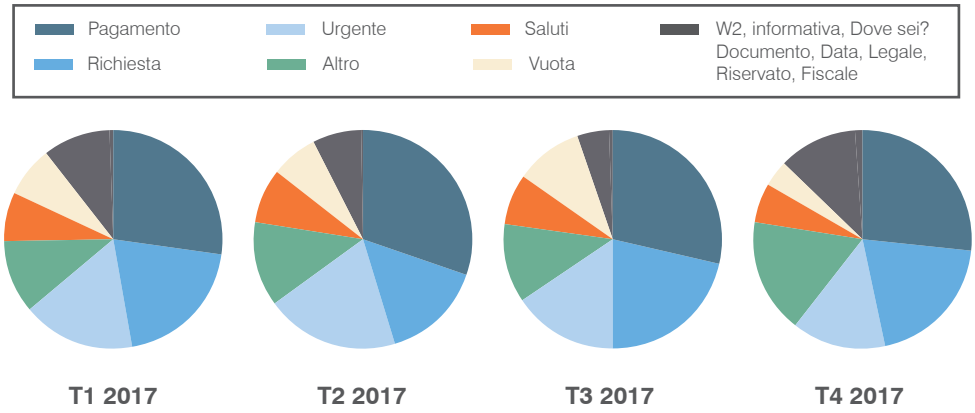
Gli aggressori colpiscono più settori
Nelle ricerche precedenti, abbiamo assistito a una diffusione più uniforme dei tentativi di frode via e-mail tra i vari settori (sebbene i settori finanziario, manifatturiero, sanitario ed energetico/delle utenze siano stati presi di mira con una frequenza leggermente più alta).

Nel T4, gli aggressori hanno puntato a nuovi settori. Nel settore immobiliare, i criminali hanno trovato nuovi modi per speculare su transazioni di alto valore. D'altro canto, nel settore dell'istruzione, gli attacchi hanno fatto un salto del 77% rispetto al trimestre precedente e del 120% rispetto all'intero anno appena trascorso.

AGGIORNAMENTO DELLE TATTICHE DI FRODE VIA E-MAIL

Per eludere gli strumenti di sicurezza tradizionali e raggiungere le proprie vittime, i truffatori modificano costantemente le proprie tecniche.

Righe dell'oggetto utilizzate nei tentativi di frode via e-mail
"Pagamento", "richiesta" e "urgente" sono le righe dell'oggetto più diffuse, ma nel T4 abbiamo assistito a un aumento delle righe dell'oggetto di ambito legale.



Frode mediante bonifico
LA FRODE MEDIANTE BONIFICO continua a essere la forma più frequente di frode via e-mail, rappresentando circa il 27% del volume di messaggi di posta elettronica fraudolenti. Generalmente, questo tipo di frode si contraddistingue dagli altri per il fatto che l'oggetto dell'e-mail contiene un sinonimo della parola "pagamento".

Truffa fiscale
LE TRUFFE FISCALI BASATE SUI MODULI W2 sono aumentate nei primi trimestri degli ultimi due anni, probabilmente a causa delle scadenze imminenti per l'invio della certificazione di reddito negli Stati Uniti. Per fare un esempio, nel T1 abbiamo assistito a un'impennata pari al 3.408% rispetto al trimestre precedente. Nel T2, una volta superate le scadenze per l'invio delle certificazioni, il volume di questi attacchi è sceso, fino a raggiungere un ritmo costante.

Cambiamento delle identità e dell'oggetto delle e-mail
Gli autori degli attacchi assumono tutta una serie di ruoli per impersonare figure autoritarie degne di fiducia. Nel corso del 2017, gli attacchi fraudolenti via e-mail sono stati caratterizzati dall'alternanza di due categorie di riga dell'oggetto: quella che includeva la parola "urgente" e quella che includeva la parola "richiesta".

"Urgente" e "richiesta"
Generalmente, i messaggi che rientrano nella categoria "urgente" sono più diretti e concisi. Quelli che, invece, includono la parola "richiesta" nella riga dell'oggetto adottano un approccio più cauto. Infatti, stabiliscono un rapporto del tipo "botta e risposta" prima di richiedere informazioni di valore.

"Legale"
Nel T4 sono emerse altre due categorie di riga dell'oggetto: quella che include una data e quella che include la parola "legale".

Per quanto si tratti ancora di una cifra irrisoria in termini assoluti, gli attacchi che rientrano nella categoria "legale" hanno conosciuto un aumento pari a 1.850% rispetto all'anno precedente. L'e-mail fraudolenta più dilagante di questa categoria è stata quella caratterizzata da una riga dell'oggetto che recitava "appuntamento telefonico con l'avvocato".

FRODE CON BONIFICO BANCARIO
Nelle frodi con bonifico bancario, il truffatore invia un'e-mail fingendosi un dirigente. L'e-mail induce il destinatario con l'inganno a effettuare un bonifico bancario sotto forma di una transazione commerciale ordinaria o di una trattativa importante che necessita di rimanere segreta.

TRUFFA W2
In questa truffa, qualcuno che finge di essere un dirigente chiede al reparto Finanze di inviare la documentazione relativa ai dipendenti. Questa documentazione verrà in seguito utilizzata per il furto di identità e altri attacchi. La truffa prende il nome dalla certificazone fiscale W2 che i datori di lavoro statunitensi utilizzano per calcolare lo stipendio di ciascun dipendente.

In questi attacchi, il truffatore tenta solitamente di spostare l'interazione e il bonifico bancario dall'e-mail al contatto telefonico. Questi attacchi vanno a buon fine in quanto il relativo autore impersona una figura autoritaria con la quale, generalmente, la vittima non collabora. Inoltre, dal momento che l'interazione avviene per lo più offline, queste truffe sono più difficili da rilevare e bloccare per i team addetti alla sicurezza.

Creazione di cronologie di e-mail false
I tentativi di frode che sfruttano cronologie di e-mail false hanno caratterizzato ogni singolo trimestre del 2017.

Questa tecnica si fonda sull'utilizzo di "Re:" o "Fwd:" nella riga dell'oggetto o di una cronologia di e-mail falsa, oppure delle due opzioni combinate. Questa catena di e-mail "artigianali" allega una cronologia di e-mail dall'aspetto realistico che suggerisce che i portatori di interessi in questione hanno già approvato la richiesta.

Nel T4, più dell'11% di tutti gli attacchi fraudolenti via e-mail includeva una versione di questa tecnica; si è verificato, dunque, un aumento del 7,3% rispetto allo stesso trimestre dell'anno precedente.

TECNICHE DI ATTACCO PRINCIPALI TRAMITE FALSIFICAZIONE DEL DOMINIO E DEL NOME VISUALIZZATO

Nel corso del 2017, il mix di messaggi fraudolenti via e-mail ha visto alternarsi la falsificazione del dominio, la falsificazione del nome visualizzato e la generazione di domini sosia (o domini "cugini").

FALSIFICAZIONE DEL DOMINIO
L'autore di questo tipo di truffa impersona colleghi o contatti di fiducia facendo apparire le e-mail come provenienti da un indirizzo attendibile.

FALSIFICAZIONE DEL NOME VISUALIZZATO
La falsificazione del nome visualizzato consiste nell'inserimento di un nome e di un indirizzo e-mail familiare nel campo "Da:" che gli utenti visualizzano sulle e-mail in arrivo. Quando il destinatario risponde, la risposta viene inviata all'indirizzo specificato nell'intestazione "R:" dell'e-mail.

DMARC
DMARC, acronimo di "Domain-based Message Authentication, Reporting and Conformance", è un protocollo di validazione dei messaggi di posta elettronica che contrasta moltepici attacchi fraudolenti via e-mail.

Falsificazione del dominio
LA FALSIFICAZIONE DEL DOMINIO, ossia una truffa che consiste nel furto dei domini e-mail affidabili di un'organizzazione da parte di criminali, continua a costituire un'ampia porzione degli attacchi fraudolenti via e-mail. Nel T4, il 69% delle organizzazioni colpite da truffe via e-mail ha subìto almeno un attacco basato sulla falsificazione del dominio. Se analizziamo, poi, l'intero 2017, quasi il 93% delle organizzazioni ha subìto un attacco di questo tipo.

Falsificazione del nome visualizzato
LA FALSIFICAZIONE DEL NOME VISUALIZZATO tramite servizi di posta elettronica basati sul Web ha costituito circa il 40% degli attacchi fraudolenti via e-mail nel T4. Aol.com e gmail.com sono stati i domini di invio preferiti per queste minacce, sebbene i responsabili degli attacchi utilizzino anche molti altri domini.

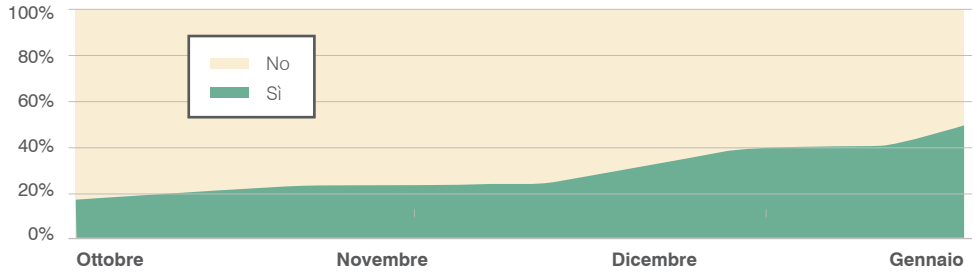
Utilizzo di DMARC
Gli attacchi basati sulla falsificazione del dominio possono essere evitati tramite l'implementazione del sistema di autenticazione delle e-mail **DMARC**. Non c'è da sorprendersi se, nel 2017, abbiamo assistito alla creazione di iniziative volte ad incrementare l'adozione di DMARC.

A ottobre, il Dipartimento della sicurezza interna degli Stati Uniti d'America ha emanato la Binding Operational Directive (Direttiva operativa vincolante) 18-01. La direttiva si propone di aumentare la sicurezza degli individui che ricevono e-mail da agenzie federali o che visitano un sito Web federale. Una parte importante della direttiva ordina a tutte le agenzie federali civili di implementare DMARC quanto prima.

Quando la direttiva è stata annunciata, quasi 1 e-mail su 8 inviate da un indirizzo e-mail .gov era fraudolenta. Soltanto il 17% circa delle agenzie aveva adottato DMARC.

90 giorni dopo il lancio dell'iniziativa, questa percentuale è più che triplicata. Quasi il 52% delle agenzie ha rispettato la prima importante scadenza in termini di adozione di DMARC.

Implementazione di DMARC tra le agenzie federali civili
Sempre più agenzie stanno adottando l'autenticazione delle e-mail sulla scia di una direttiva federale. Eppure, quasi la metà di esse non ha ancora raggiunto questa prima importante tappa.



Poco dopo l'annuncio della direttiva, il National Health Information Sharing and Analysis Center (NH-ISAC), un'associazione di categoria che aiuta gli operatori sanitari a condividere informazioni sulla sicurezza, ha chiesto ai relativi membri di impegnarsi a distribuire DMARC nel 2018.

UNO SGUARDO PIÙ APPROFONDITO AI DOMINI SOSIA

GENERAZIONE DI DOMINI SOSIA
La generazione di domini sosia consiste nella registrazione di nomi di dominio apparentemente simili a quelli di marchi affidabili da parte dei truffatori.

LA GENERAZIONE DI DOMINI SOSIA, la quale consiste nella registrazione di un dominio ingannevolmente simile a un dominio affidabile da parte del truffatore, rappresenta un'altra tattica efficace. Gli autori degli attacchi inducono le persone con l'inganno a fornire informazioni riservate tramite e-mail che sembrano provenire da persone a noi familiari.

Gli autori degli attacchi architettano questi domini impostori apportando modifiche quasi impercettibili al dominio originale. Possono ricorrere allo scambio di singoli caratteri, come ad esempio il numero 0 invece della lettera O, oppure possono optare per l'inserimento di caratteri, come l'aggiunta di una S alla fine del dominio.

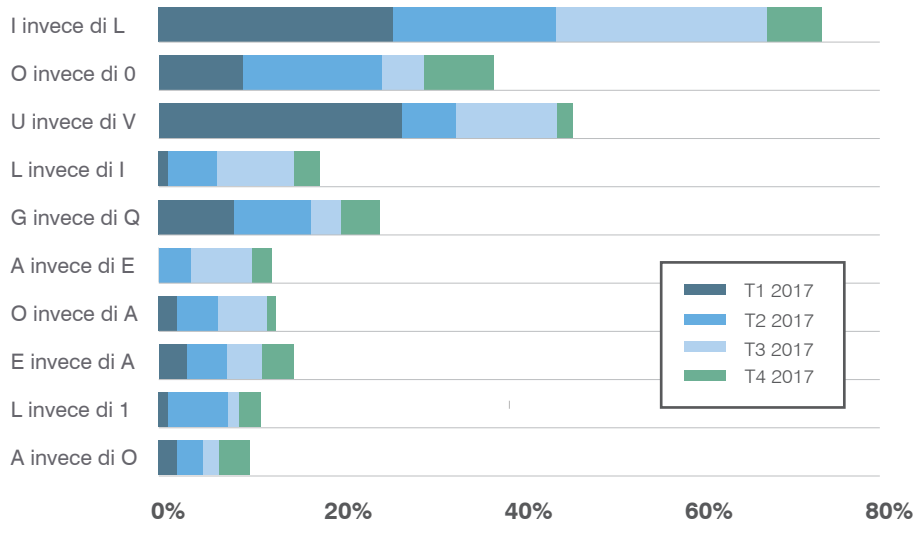
Il volume degli attacchi lanciati da domini sosia non è elevato quanto quello degli attacchi basati sulla falsificazione del dominio e del nome visualizzato. Questa differenza è forse giustificata dal fatto che, perché la tecnica funzioni, il truffatore deve registrare un dominio, la qual cosa ha un costo. Tuttavia, dal momento che un singolo nome di dominio affidabile può avere infinite variazioni simili, i truffatori hanno svariate possibilità per lanciare tali attacchi.

Scambio di caratteri

Alla stregua delle altre tattiche di frode via e-mail, le tecniche di attacco tramite domini sosia cambiano ogni trimestre. Analizzando il 2017, lo scambio dei singoli caratteri è stata la tecnica più diffusa, utilizzata circa il 38% delle volte. Gli scambi di lettere più comuni sono stati:

- Una L al posto di una I (17,4%)
- Il numero 0 invece della lettera O (8,7%)
- Una V al posto di una U (8%)

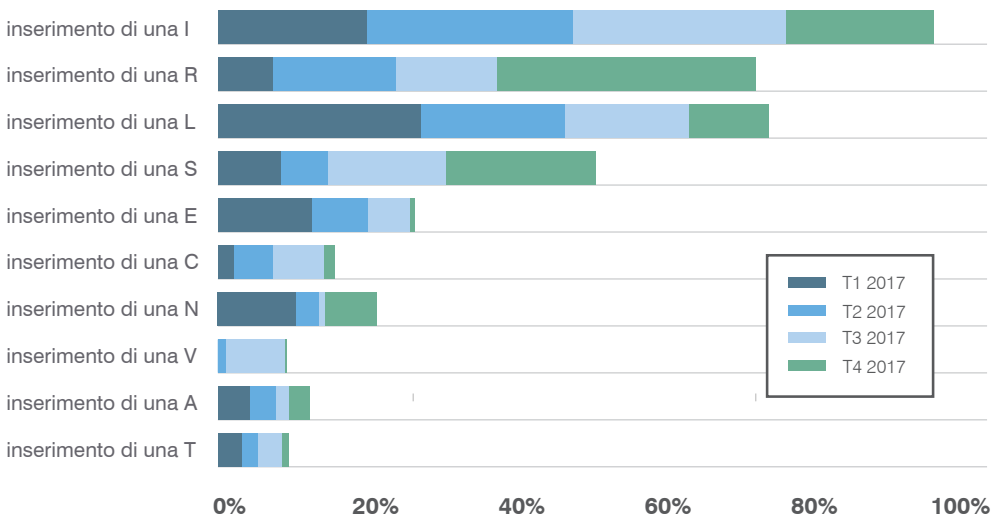
Scambio dei caratteri nei domini sosia
Dal momento che alcuni caratteri si assomigliano tra loro, i truffatori dispongono di più opzioni per creare domini simili a quelli affidabili.



Inserimento di caratteri
I domini impostori dotati di un carattere aggiuntivo sono stati utilizzati circa il 34% delle volte nel corso dell'anno. Le aggiunte più comuni sono state:

- Una I (23,7%)
- Una R (19,3%)
- Una L (15,4%)

Inserimento di caratteri aggiuntivi nei domini sosia
Essendo difficile rilevare i caratteri aggiuntivi negli indirizzi e-mail, la propagazione di nuove variazioni di domini e-mail sicuri non conosce limiti.



Altre tecniche
Un'altra tecnica popolare consiste nell'aggiunta o rimozione del carattere iniziale o finale del dominio. Questo approccio è stato utilizzato da circa il 13% dei domini sosia registrati.

Fra le altre tattiche utilizzate per la generazione di domini sosia vanno ricordate:

- Inserimento del trattino
- Rimozione di caratteri
- Utilizzo di refusi e **OMOGRAFI**

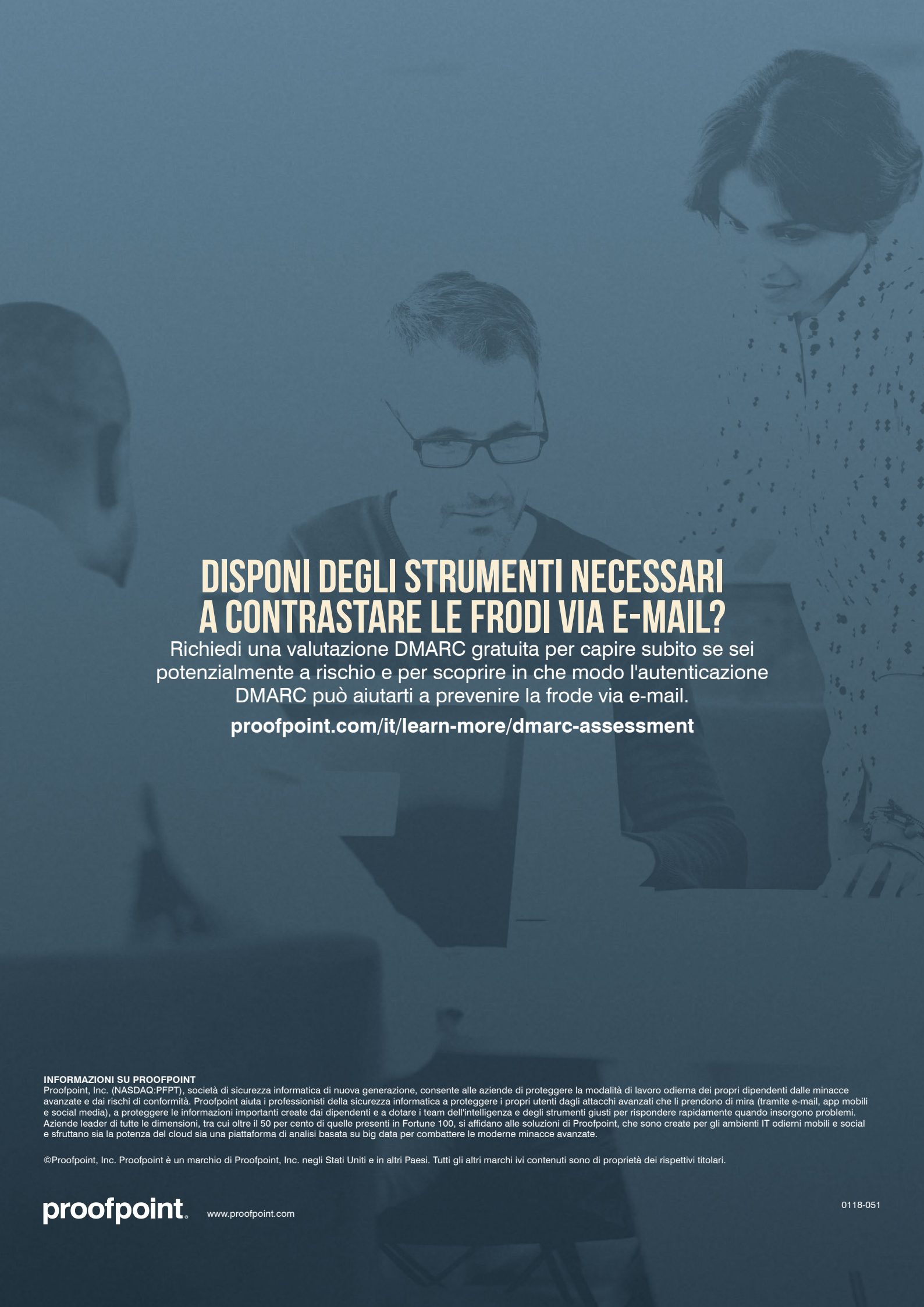
ATTACCO OMOGRAFICO
L'attacco omografico combina set di caratteri di diverse lingue per creare domini sosia che vengano visualizzati come identici dall'essere umano, pur essendo di fatto diversi per un computer. Per esempio, un dominio non sicuro che utilizza la lettera A dell'alfabeto cirillico apparirà come identico a un dominio sicuro che utilizza la lettera A dell'alfabeto latino.

CONCLUSIONE E CONSIGLI

Malgrado gli ingenti investimenti delle organizzazioni nella sicurezza, la frode via e-mail è in crescita. I criminali informatici utilizzano tecniche sempre più avanzate. Essi evadono le soluzioni di sicurezza tradizionali, trasformando così i dipendenti nell'ultima linea di difesa.

Le tattiche di frode via e-mail cambiano continuamente. Per questo motivo, le organizzazioni necessitano di una difesa a più strati che includa:

1. **Autenticazione delle e-mail DMARC**. Blocco di tutti gli attacchi di impostori che falsificano domini e-mail affidabili.
2. **Classificazione dinamica**. Analisi del contenuto e del contesto delle e-mail finalizzata a contrastare le tattiche di falsificazione del nome visualizzato e di generazione dei domini sosia sul proprio gateway e-mail.
3. **Riconoscimento dei domini sosia.** Identificazione e segnalazione di domini potenzialmente rischiosi operate da terzi.
4. **Prevenzione della perdita dei dati.** Prevenzione dell'uscita dei propri dati sensibili, quali quelli relativi al W2, dal proprio ambiente.



DISPONI DEGLI STRUMENTI NECESSARI A CONTRASTARE LE FRODI VIA E-MAIL?

Richiedi una valutazione DMARC gratuita per capire subito se sei potenzialmente a rischio e per scoprire in che modo l'autenticazione DMARC può aiutarti a prevenire la frode via e-mail.

proofpoint.com/it/learn-more/dmarc-assessment

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.

proofpoint. www.proofpoint.com