proofpoint.

C'è posta (compromessa) per te!

Riepilogo delle 10 più grandi, più audaci e più sfrontate truffe con violazione dell'email aziendale del 2020 e del 2019

INTRODUZIONE

Farsi ingannare da un'email fraudolenta è più facile di quanto si possa pensare. Ciò si deve al fatto che gli attacchi di violazione dell'email aziendale (Business Email Compromise, BEC) si approfittano della natura umana, dei tratti psicologici innati e comuni a tutti. Questo è un riepilogo degli attacchi BEC ed EAC più noti e più devastanti degli ultimi 12 mesi.

Non è difficile capire perché gli attacchi BEC funzionino. Richieste provenienti da persone legittime, richieste di bonifici o di informazioni sensibili sui dipendenti, possono far parte della normale giornata di lavoro. Ma quando tali richieste provengono da qualcun altro, può trattarsi di uno scambio di identità, dalle conseguenze costose.

Il problema è che non è sempre facile cogliere la differenza fra le email autentiche e la truffa di un impostore.

Questo perché gli attacchi BEC sfruttano le qualità intrinseche che contraddistinguono le persone, che fanno andare avanti la società e gli affari. I truffatori che utilizzano gli attacchi BEC si approfittano della psicologia umana e dei processi aziendali per indurre gli utenti a effettuare bonifici, a dirottare stipendi e pagamenti, a inviare informazioni sensibili e altro ancora.

La violazione degli account email (Email Account Compromise, EAC) è un attacco parente stretto della BEC, ma invece di limitarsi a impersonare qualcuno di cui l'utente si fida tramite un account simile, i criminali informatici che utilizzano questo tipo di attacco si impossessano dell'account reale della persona di fiducia.

Non sorprende che le truffe BEC abbiano già sottratto miliardi di dollari alle loro vittime, e il ritmo sta accelerando. Ecco alcune delle truffe più grandi, più audaci e più sfrontate denunciate nei mesi recenti.

1. Barbara Corcoran di "Shark Tank"

L'emittente televisiva ABC descrive le stelle del suo spettacolo di successo "Shark Tank" come "risoluti magnati multimilionari e miliardari che si sono fatti da sé", ma ciò non significa che non possano essere beffati.

A febbraio Barbara Corcoran, una dei giudici del programma, che decide se investire nei sogni di aspiranti imprenditori, è stata alleggerita di quasi 400.000 dollari da una truffa BEC.

La Corcoran, che ha fatto fortuna come mediatore immobiliare, a fine febbraio 2020 ha ammesso che la sua contabile ha inviato i soldi a una persona che si spacciava per assistente della Corcoran stessa e che affermava di dover pagare la ristrutturazione di una proprietà. Dopo l'invio del denaro la Corcoran si è resa conto del fatto che l'indirizzo di posta elettronica non era affatto quello dell'assistente: la differenza era una lettera in meno.

"Non c'era motivo di avere sospetti poiché investo molto in immobili", ha raccontato la Corcoran alla rivista *People*.[1]

In seguito il personale informatico della Corcoran ha ricondotto l'attacco a un indirizzo IP cinese.

Il denaro è stato poi restituito. Dato che il bonifico era passato per una banca tedesca prima di giungere al conto cinese del truffatore[2], la banca della Corcoran ha fatto pressione su quella tedesca per congelare i soldi, dandole il tempo di provare che si trattava di una frode.

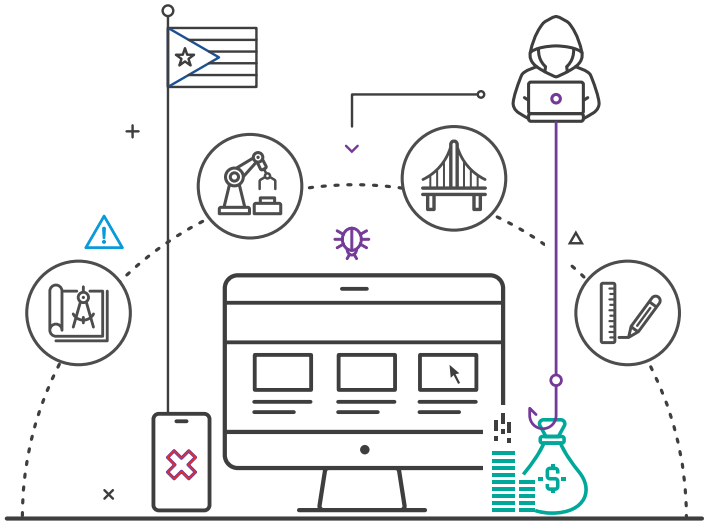
Che un messaggio di email sembri consueto, e quindi non sospetto, è una delle principali caratteristiche intrinseche degli attacchi BEC.

[1] Robyn Merrett, People. "Shark Tank's Barbara Corcoran Gets Back $388K Stolen in Phishing Scam: 'I'm Thrilled!'"
(A Barbara Corcoran di Shark Tank vengono restituiti 388.000 dollari rubati a seguito di un truffa di phishing: sono entusista!) Marzo 2020.

[2] Ibid.

2. Portorico

Di recente Portorico ha sofferto diverse calamità, fra cui uragani, la crisi di debito del governo e una recessione, a cui ora si sono aggiunti gli attacchi BEC.



$4 milioni

persi in tre distinti attacchi BEC

A gennaio Portorico ha perso oltre 4 milioni di dollari in tre distinti attacchi BEC sferrati contro agenzie governative[3].

La truffa è iniziata un mese prima, con la violazione del computer di un addetto alle finanze del Sistema Pensionistico portoricano. Usando l'account del dipendente, il criminale informatico ha inviato delle email ai dipendenti delle altre agenzie. Le email chiedevano ai destinatari di modificare il numero di conto corrente legato ai pagamenti.

Tecnicamente, questo attacco in stile BEC è in realtà un esempio di violazione dell'account email (EAC). Infatti l'aggressore non si è limitato a rendere verosimile il proprio indirizzo email, ma ha usato un account legittimo.

Il furto più grande è stato quello ai danni dell'Azienda di Sviluppo Industriale di Portorico, un'impresa pubblica che investe nello sviluppo economico dell'isola, con la perdita di 2,6 milioni di dollari in fondi governativi[4] . L'Azienda Turistica Portoricana a sua volta è stata derubata di 1,5 milioni di dollari, mentre l'Azienda Commercio ed Esportazioni ne ha persi 63.000.

Come nella maggior parte degli attacchi BEC, la vulnerabilità di Portorico è legata alla natura umana.

"L'enorme errore del governo è stato nelle procedure, non nella tecnologia", ha dichiarato alla Associated Press José Quiñones, presidente di Obsidis Consortia, un'organizzazione no profit portoricana dedicata alla sicurezza informatica[5].

[3] Dánica Coto (Associated Press). "3 employees suspended in $4M Puerto Rico online scam" (Sospesi 3 dipendenti coinvolti in una truffa online del valore di 4 milioni di dollari a Portorico). Febbraio 2020.

[4] Dánica Coto (Associated Press). "Official: Puerto Rico govt loses $2.6M in phishing scam" (Ufficiale: il governo di Portorico perde 2,6 milioni di dollari in una truffa di phishing). Febbraio 2020.

[5] Dánica Coto (Associated Press). "3 employees suspended in $4M Puerto Rico online scam" (Sospesi 3 dipendenti coinvolti in una truffa online del valore di 4 milioni di dollari a Portorico). Febbraio 2020.

3. Nikkei

Nikkei, il gigante giapponese dei media, non corrisponde allo stereotipo della tipica vittima di una frode finanziaria.

SI tratta di uno dei più grandi gruppi giapponesi della comunicazione, possiede il *Financial Times* di Londra oltre a dare il suo nome all'indice della Borsa di Tokyo.

Le sue enormi dimensioni e il peso finanziario ne fanno un bersaglio particolarmente appetibile per i truffatori. Nel settembre 2019 un dipendente della sua filiale statunitense, Nikkei America, ha trasferito 29 milioni di dollari seguendo le istruzioni di un'email che sembrava provenire da un dirigente esecutivo della casa madre.

Sfortunatamente, l'email proveniva da una persona che si spacciava per quel dirigente (secondo altre fonti l'hacker avrebbe compromesso l'account stesso del dirigente[6], il che definirebbe l'attacco come EAC. L'azienda e le autorità hanno reso pubblici pochi dettagli).

I funzionari di Nikkei hanno dichiarato che il gigante della comunicazione avrebbe tentato di recuperare il denaro, ma non è chiaro se il tentativo abbia avuto successo.[7]

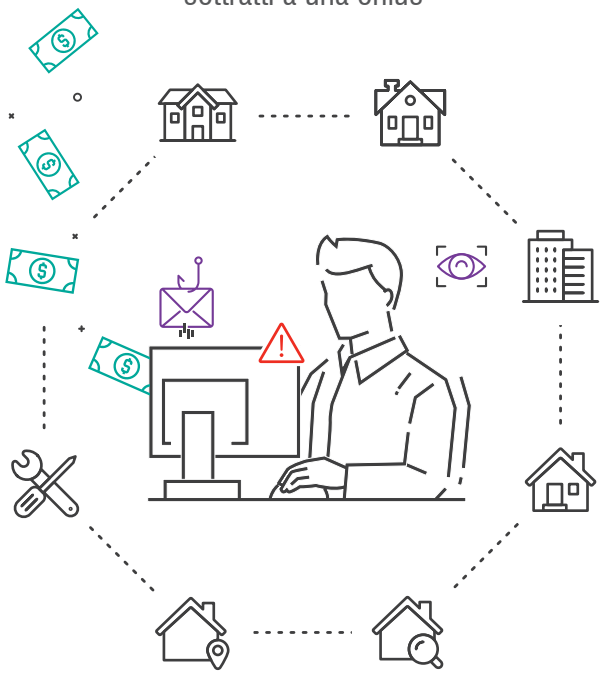
[6] Lindsey O'Donnell (ThreatPost). "BEC Scam Costs Media Giant Nikkei $29 Million" (Una truffa BEC costa al gigante dei media Nikkei 29 milioni di dollari). Novembre 2019.

[7] Nikkei. "Matter concerning transfer of funds at Nikkei Inc.'s US subsidiary" (Questioni relative al trasferimento di fondi presso la filiale statunitense della Nikkei Inc.). Ottobre 2019.

4. Red Kite Community Housing

$1,2 milioni

sottratti a una onlus



Le persone che hanno difficoltà a pagarsi un alloggio in High Wycombe, una cittadina britannica fuori Londra, possono rivolgersi alla Red Kite Community Housing. Questa società no profit di edilizia popolare possiede e gestisce nell'area di Wycombe oltre 6.500 abitazioni, che affitta ai poveri per canoni inferiori a quelli di mercato.

Purtroppo Red Kite ha subito essa stessa una perdita finanziaria dopo essere stata colpita da un attacco BEC nell'agosto 2019. Gli autori dell'attacco hanno rubato 932.000 sterline (1,2 milioni di dollari).

Secondo gli organi di stampa, i criminali informatici hanno impersonato uno dei fornitori di Red Kite registrando un dominio fotocopia. Usando il dominio fasullo, che somigliava molto a quello del fornitore vero, i criminali informatici hanno indotto il destinatario a inviare soldi al loro conto corrente. Il corpo dell'email conteneva una cronologia fittizia di messaggi per farla sembrare parte di una lunga conversazione intercorsa fra i dirigenti esecutivi di Red Kite e il fornitore[8].

Le misure di sicurezza di Red Kite includevano l'autenticazione a due fattori per verificare le modifiche a pagamenti e conti correnti, ha dichiarato un portavoce di Red Kite al sito web scozzese di notizie tecnologiche *Digit*.[9]

Red Kite afferma che i suoi sistemi non sono stati compromessi. Il punto debole? Un errore umano. Il dipendente di Red Kite è stato tratto in inganno da un'email e non ha seguito le normali procedure .

"È questo unico errore che abbiamo affrontato nella revisione interna di apprendimento e dei necessari cambiamenti da tradurre in azione", ha affermato l'associazione[10].

Red Kite ha segnalato la violazione ai propri inquilini (che non hanno dovuto accollarsi il costo del furto), alla polizia locale, a una società esterna esperta in analisi forensi informatiche e all'agenzia locale di regolamentazione degli alloggi popolari[11].

Da allora la onlus ha aggiornato il proprio piano per la sicurezza, ha completato una verifica ed esaminato i propri sistemi e processi di pagamento, oltre ad aver messo in atto ulteriori misure di sicurezza, come la formazione del personale.

[8] Lucie Heath *(Inside Housing)*. "Housing association defrauded of nearly £1m after falling victim to cyber scam" (Associazione per l'edilizia popolare defraudata di quasi 1 milione di sterline dopo essere caduta vittima di una truffa informatica). Gennaio 2020.

[9] David Paul, *(Digit)*. "British Charity Loses almost £1m in Domain Spoofing Scam" (Ente benefico inglese perde quasi 1 milione di sterline in una truffa di spoofing del dominio). Febbraio 2020.

[10] Red Kite Community Housing. https://redkitehousing.org.uk/

[11] Tara Seals *(ThreatPost.com)*. "Community Housing Nonprofit Hit with $1.2M Loss in BEC Scam." (Associazione no profit per l'edilizia popolare subisce una perdita di 1,2 milioni di dollari a causa di una truffa BEC). Febbraio 2020.

5. Membri delle congregazioni di templi ebraici e sinagoghe

53%

gli interpellati dalla Secure Community Network che hanno subito attacchi BEC

Uno degli elementi centrali degli attacchi BEC è che, per il destinatario, il mittente dell'email sembri qualcuno che conosce, di cui si fida e che rispetta. Normalmente si tratta di un collega, un socio d'affari o un capo. Per molti ebrei degli Stati Uniti, le autorità affidabili includono anche la figura del rabbino del proprio tempio o sinagoga.

In una nuova versione del vecchio trucco del buono regalo, un criminale informatico o gruppo di hacker ha preso di mira i fedeli dell'area metropolitana di Detroit, della Baia di San Francisco, dell'Idaho, del Tennessee e di altre congregazioni nel resto del paese. Spacciandosi per il rabbino locale, i truffatori hanno chiesto ai destinatari di acquistare dei buoni regalo, fingendo una raccolta di fondi.

Tre membri di una sinagoga in Virginia hanno risposto alle email, pensando che provenissero dal loro rabbino, acquistando buoni regalo per un totale di 2.500 dollari. Finora due delle tre vittime sono riuscite a far annullare i buoni e a ottenere la restituzione dei soldi.

Nell'Idaho una donna ha perso 400 dollari nella stessa truffa. Per fortuna, proprio mentre stava per inviare all'indirizzo email del presunto "rabbino" i codici dei buoni, insieme al numero di conto e al PIN, un cassiere si è reso conto di cosa stava per fare e l'ha fermata[12].

"Questa grave truffa funziona proprio perché i membri della congregazione si fidano del proprio ministro di culto", ha affermato il rabbino Debra Newman Kamin, presidente dell'Assemblea Rabbinica, organizzazione professionale dei rabbini del movimento Conservatore.[13]

Anche se l'FBI e la Federal Trade Commission hanno avvisato la popolazione delle truffe dei buoni regalo in generale, l'ondata di tali trucchi a danno delle congregazioni ebraiche ha fatto scattare la risposta della Secure Community Network (SCN), l'iniziativa di sicurezza interna nazionale della comunità degli Ebrei Nordamericani.

La SCN ha segnalato che nel 2019, il 53% delle organizzazioni interpellate (comprendenti ogni sorta di aziende, enti locali e gruppi religiosi) aveva subito un attacco informatico. Si tratta di un aumento del 38% rispetto all'anno precedente.

[12] Ari Feldman *(Forward)*. "'Rabbi' gift card scam spurred congregants to spend thousands" (La truffa dei buoni regalo del rabbino ha spinto i fedeli a spendere migliaia dollari). Febbraio 2020.

[13] Rabbi Jason Miller *(The Jewish News)*. "Email Spoofing Scam Targets Rabbis and Congregants in Metro Detroit" (Una truffa di spoofing dell'email colpisce rabbini e fedeli nell'area metropolitana di Detroit). Febbraio 2020.

6. Distretto Scolastico Indipendente di Manor

Negli ultimi mesi un'ondata di attacchi informatici ha colpito negli Stati Uniti piccole città, agenzie locali e distretti scolastici. Gli hacker forse danno per scontato che piccole agenzie locali, a volte a corto di fondi, abbiano meno soldi da dedicare alla sicurezza informatica rispetto alle giurisdizioni più grandi o al settore privato. In molti casi hanno ragione.

Ma questa è solo una parte del problema. Sia nelle aziende piccole come in quelle grandi, l'anello debole della sicurezza sono solitamente le persone.

$2,3 milioni

rubati in un solo attacco BEC

Un esempio: il Distretto Scolastico Indipendente di Manor nelle vicinanze di Austin, in Texas. Nel novembre 2019 questo distretto di 9.600 studenti è stato derubato di 2,3 milioni di dollari tramite un attacco BEC.

Da novembre 2019 e per alcuni mesi il truffatore ha inviato email a diversi dipendenti del distretto, cambiando le istruzioni di pagamento per un fornitore. Solo un dipendente ha abboccato, ma è stato sufficiente per creare un danno. Prima che qualcuno avesse dei sospetti, i truffatori erano riusciti a eseguire tre distinte transazioni.[14]

Il distretto spera di recuperare 800.000 dollari tramite l'assicurazione, ma la perdita netta sarà comunque di 1,5 milioni di dollari.

[14] Drew Knight, Luis de Len, KVUE-TV. "Manor ISD loses $2.3 million in phishing scam; police and FBI investigating" (Distretto scolastico indipendente di Manor perde 2,3 milioni di dollari in una truffa di phishing: polizia e FBI indagano). Gennaio 2020.

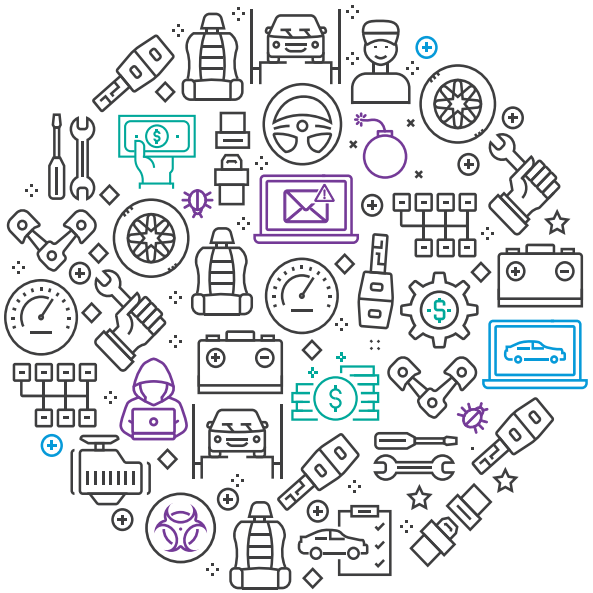
7. Toyota Boshoku

I criminali informatici che utilizzano gli attacchi BEC colpiscono aziende grandi e piccole. Negli ultimi mesi una delle vittime più grandi di uno di questi colpi è Toyota Boshoku. Alla filiale della Toyota, che fornisce i sedili e altri componenti per gli interni, nell'agosto del 2019 sono stati estorti 37 milioni di dollari.

Secondo quanto riferito dagli organi di stampa, si è trattato di un attacco BEC da manuale. L'hacker, spacciandosi per un partner commerciale dell'azienda, ha inviato delle email all'ufficio amministrazione e contabilità richiedendo un pagamento sul proprio conto corrente[15].

L'azienda afferma di aver individuato la frode velocemente, di averla denunciata alle autorità e di essere al lavoro per recuperare i soldi.

Questo attacco da 37 milioni di dollari illustra il modo in cui il social engineering può eludere anche le difese informatiche meglio finanziate, perché punta alle persone, non all'infrastruttura.

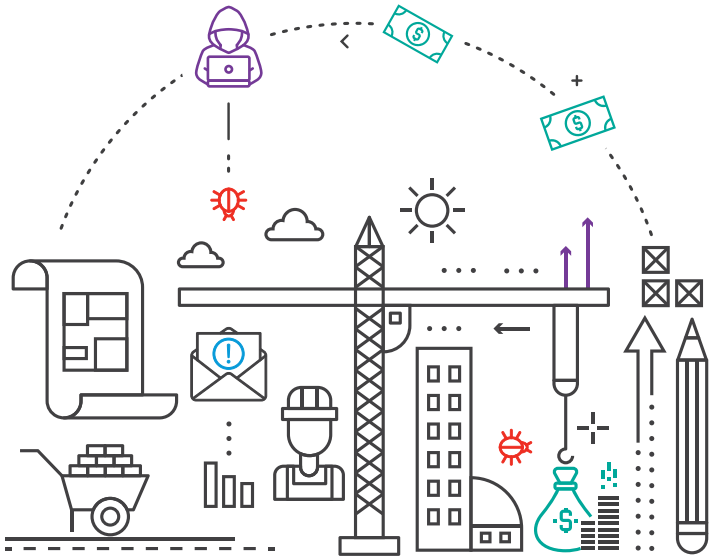


$37 milioni

rubati nel più grande attacco BEC mai denunciato

[15] Nicole Lindsey *(CPO Magazine)*. "Toyota Subsidiary Loses $37 Million Due to BEC" (Filiale di Toyota perde 37 milioni di dollari a causa di un attacco BEC). Settembre 2019.

8. Contea di Cabarrus, Carolina del Nord



$2,5 milioni

rubati usando una documentazione fasulla per un bonifico bancario

A fine 2018 la Contea di Cabarrus aveva orgogliosamente annunciato il piano di costruzione di una nuova scuola superiore da 2,5 milioni di dollari, la West Cabarrus High. A quanto pare, la cosa non è sfuggita ai criminali informatici.

Durante la costruzione a novembre, il distretto scolastico ha ricevuto un'email apparentemente proveniente dall'appaltatore incaricato di costruire la scuola. L'email includeva un nuovo conto corrente per il trasferimento elettronico dei fondi all'appaltatore, con le autorizzazioni firmate e altra documentazione. Qualche settimana dopo il distretto ha effettuato il bonifico nel nuovo conto come da istruzioni.

Nulla è sembrato strano fino a gennaio, quando i funzionari hanno ricevuto dall'appaltatore un avviso di mancato pagamento.

Hanno quindi capito che il contenuto dell'email (i dati del conto, i documenti e le firme) era fasullo. Il distretto è riuscito a recuperare 776.518,40 dollari. I rimanenti 1.728.082,60 dollari sono spariti, riallocati e riciclati tramite una rete di conti correnti secondari[16].

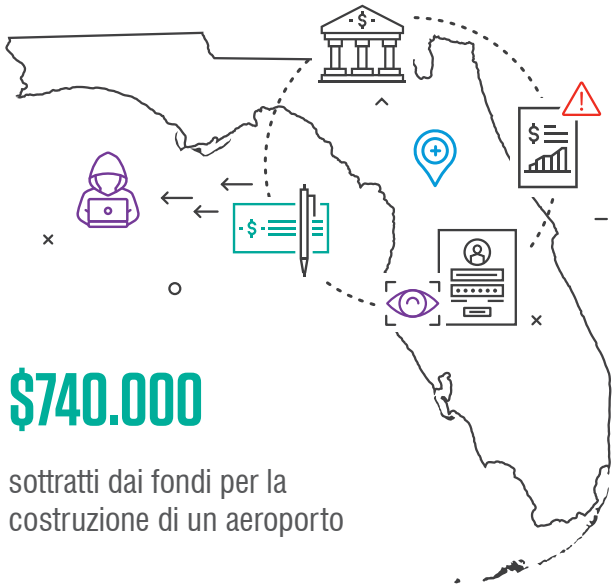
I Commissari della Contea di Cabarrus hanno rispettato il programma di costruzione attingendo i soldi mancanti a un fondo speciale creato per "circostanze straordinarie".[17]

Ultimo aggiornamento dalla contea: "L'indagine continua".

[16] Ionut Arghire (SecurityWeek). "Scammers Grab $2.5 Million From North Carolina County in BEC Scam" (Truffatori si appropriano di 2,5 milioni di dollari della Contea della Carolina del Nord a seguito di una truffa BEC). Agosto 2019.

[17] Cabarrus County. "Cabarrus County Government targeted in social engineering scam" (L'amministrazione della Contea di Cabarrus colpita da una truffa di social engineering). Agosto 2019.

9. Ocala, Florida



$740.000

sottratti dai fondi per la costruzione di un aeroporto

Gli analisti della sicurezza informatica possono aggiungere Ocala (località della Florida che non arriva a 60.000 abitanti), all'elenco di piccole cittadine americane colpite dai criminali informatici.

Nel settembre del 2019 la città è stata derubata di oltre 740.000 dollari in un attacco BEC che ha puntato a un vicino terminal aeroportuale in costruzione.

Come la maggior parte degli attacchi BEC, anche questo è iniziato con un'email diretta al capo contabile della municipalità, messaggio apparentemente proveniente da un commercialista dell'impresa edile che stava lavorando al progetto.

Il messaggio includeva un modulo della municipalità stessa contenente la richiesta di cambiare le coordinate bancarie dell'impresa. Il modulo riportava un codice di instradamento e il numero del nuovo conto corrente e, per dare un tocco di verosimiglianza, la copia di un assegno nullo proveniente dal conto[18].

L'amministrazione cittadina ha capito di essere stata truffata solo dopo che la vera impresa edile ha inviato la fattura il 17 ottobre. La fattura è stata pagata il giorno dopo, ma sul conto del truffatore. Qualche giorno dopo l'impresa edile ha segnalato di non aver ricevuto i soldi[19].

Il dipendente municipale che aveva autorizzato il bonifico ha lasciato il lavoro subito dopo che la truffa è stata scoperta [20] ma di fatto chiunque avrebbe potuto farsi trarre in inganno.

L'email aveva usato il nome di un ex dipendente dell'impresa edile e un dominio email fotocopia a cui mancava una sola "s" rispetto al dominio reale[21]. Un'altra municipalità della Florida, la Città di Naples, aveva perso 700.000 dollari in un simile attacco BEC nell'agosto precedente.

I funzionari di Ocala hanno denunciato il fatto all'assicurazione per recuperare una parte del denaro, ma l'indagine è ancora in corso[22].

[18] Carlos E. Medina (Ocala StarBanner). "Ocala police: Scammers swiped nearly $750,000 from city" (La polizia di Ocala: truffatori rubano 750.000 dollari alla città). Ottobre 2019.

[19] Ibid.

[20] Ibid.

[21] S. Rowe (Dipartimento di Polizia di Ocala). "Relazione sul caso, reato: 201900183389." Ottobre 2019.

[22] WESH 2 News. "Police: Scammers swindled nearly $750,000 from city of Ocala" (La polizia: truffatori sottraggono circa 750.000 dollari alla città di Ocala). Ottobre 2019.

10. Rijksmuseum Twenthe

Per rubare denaro tramite le truffe BEC ed EAC i criminali informatici si concentrano sui potenziali obiettivi più redditizi, per cui truffano banche, grandi aziende, agenzie governative e altri. Quindi non sorprende che prendano di mira mercanti d'arte e musei, che commerciano in capolavori di grande valore.

Il Rijksmuseum Twenthe, museo nazionale di Enschede, nei Paesi Bassi, ha perso 3,1 milioni di dollari a causa di un truffatore che utilizzando la tecnica di attacco EAC si è spacciato per un rinomato mercante d'arte londinese. Per mesi il museo aveva trattato tramite email con il mercante per acquistare il dipinto del 1824 "A View of Hampstead Heath: Child's Hill, Harrow in the Distance" del paesaggista inglese John Constable.[23]

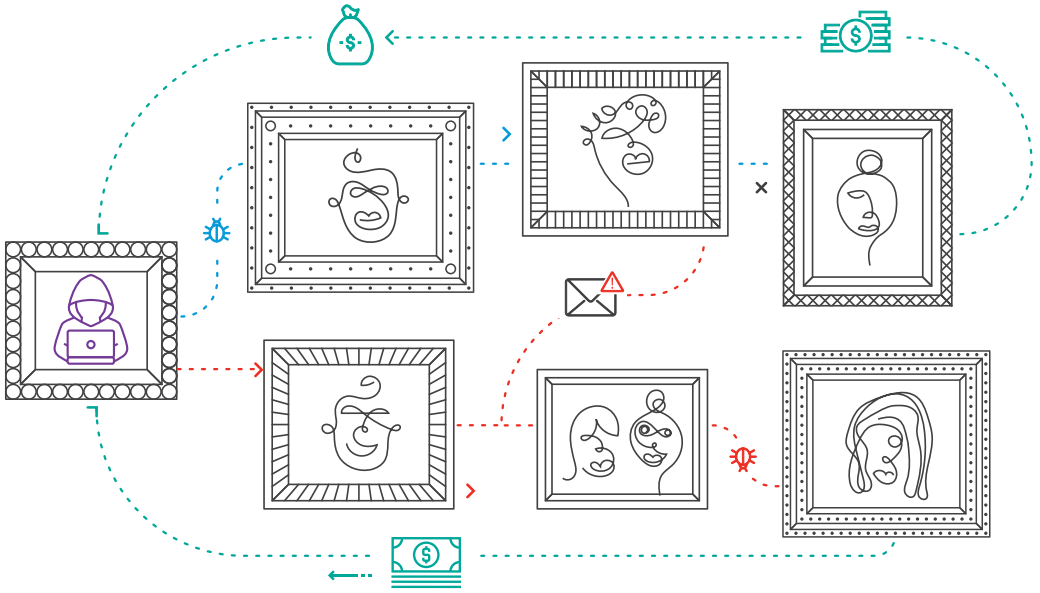
A un certo punto delle trattative, il truffatore ha assunto il controllo dell'account email del mercante oppure ne ha creato uno falso e convincente (i dettagli sono oggetto della causa in corso) e poi ha atteso la chiusura della vendita. Il mercante ha spedito il dipinto, ma quando si è trattato di pagare, il museo ha effettuato il bonifico verso un conto corrente di Hong Kong, non quello del venditore. Il truffatore aveva "aggiornato" i dati per il pagamento in un'email precedente.

Il museo sta facendo causa al mercante, accusandolo di negligenza per non aver notato o non essere intervenuto quando il truffatore ha violato il suo account. Il mercante ha intrapreso le vie legali a sua volta, asserendo che era il museo a dover verificare le coordinate bancarie prima di effettuare il pagamento.

Per adesso il museo trattiene il dipinto mentre la causa continua.

$3,1 milioni

sottratti da un finto mercante d'arte



[23] Ellen Milligan (Bloomberg). "Fraudsters Posing as Art Dealer Got Gallery to Pay Millions" (Truffatori si spacciano per mercanti d'arte e inducono una galleria a pagargli milioni). Gennaio 2020.

CONCLUSIONI E RACCOMANDAZIONI

Come mostrano questi casi, gli attacchi BEC ed EAC sono truffe dalle pari opportunità: colpiscono aziende di ogni dimensione e persone di qualsiasi livello gerarchico.

Gli attacchi BEC ed EAC sono difficili da rilevare e prevenire, soprattutto con strumenti obsoleti, prodotti singoli e difese native delle piattaforme cloud. Non si avvalgono di malware né di URL dannosi che possano essere analizzati con le difese informatiche standard.

Per fortuna non è mai troppo tardi, né troppo presto, per cominciare a sviluppare una robusta strategia di difesa dalle truffe BEC/EAC. Dato che tali attacchi si concentrano sulla fragilità umana piuttosto che sulle vulnerabilità tecniche, serve una difesa incentrata sulle persone che possa prevenire, rilevare e rispondere a un'ampia gamma di tecniche BEC ed EAC.

Informati sugli attacchi BEC/EAC e scopri come puoi bloccarli visitando il sito **proofpoint.com/us/solutions/bec-and-eac-protection.**

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0503-001-01-01 04/20