III) Fattore umano e ingegneria sociale.

Tipologie criminali “di primo livello”

BEC (Business Email Compromise e

MITM (Man in the Middle). -

Frodi finanziarie tecnologicamente avanzate :

MITB (Man In The Browser)

Analisi di casi concreti

BEC

Ancora più vicina al concetto di “social engineering”, è una truffa assai diffusa e denominata **BEC (Business Email Compromise).**

Riguarda le email aziendali che finti CEO inviano alle loro prime linee (I collaboratori più vicini), generalmente per chiedere di eseguire transazioni finanziarie come bonifici o ricariche di carte di cradito.

BEC

Eccone una tipica *:*

“Ho bisogno che mi aiuti ad acquistare buoni regalo fisici dal negozio per clienti specifici. Puoi farlo in 15 minuti? Fammi sapere se puoi così posso inviarti le informazioni necessarie sulla carta regalo e l’importo esatto.

Sono attualmente in riunione e non posso rispondere alle chiamate, quindi comunichiamo via e-mail.

Rimborserò i soldi oggi, ma mi servono subito i buoni regalo

BEC

Altro modello tipico di messaggio di truffa su larga scala apparentemente proveniente da un AD:

“Good morning

How are you doing today? Well, I’ve a request for you to handle. Are you available at moment?

Do have a great ahead!!!

Best regards

(CEO) “

Nel vasto panorama delle minacce alla sicurezza informatica, gli attacchi di tipo BEC sono tra i più subdoli e dannosi.

Questi attacchi si verificano quando un malintenzionato riesce a prendere il controllo di un account e-mail aziendale legittimo, utilizzandolo per perpetrare frodi.

Il modus operandi tipico può includere l'invio di fatture false ai clienti dell'azienda, oppure la richiesta ai colleghi di trasferire fondi su conti bancari controllati dagli hacker.

Gli attacchi di tipo BEC sono pericolosi per vari motivi.

Innanzitutto, poiché provengono da un account e-mail legittimo, possono essere molto difficili da rilevare: le tecniche tradizionali di filtraggio delle e-mail spesso non riescono a bloccare queste comunicazioni fraudolente.

Inoltre, dato che gli attacchi di tipo BEC si basano sulla manipolazione della fiducia e sull'inganno, possono essere particolarmente efficaci.

Ad esempio, un dipendente potrebbe non sospettare nulla di strano in una richiesta di pagamento inviata dal suo supervisore.

Gli attacchi di tipo BEC possono avere conseguenze devastanti per le aziende.

Oltre alle perdite finanziarie dirette, le aziende colpite da questi attacchi possono subire danni alla reputazione e alla fiducia dei clienti. Inoltre, possono anche dover affrontare costi legali e di risarcimento significativi se i dati dei clienti vengono compromessi.

BEC Fraud Dimensioni

BEC Fraud . Secondo Verizon, questo tipo di frode è stato il secondo attacco di social engineering più comune del 2021.

L'FBI segnala che gli attacchi BEC sono costati alle aziende statunitensi più di 12 miliardi di dollari tra il 2014 e il 2019.

BEC Dimensioni e gravità

Secondo il **report Security predictions for 2023 di Trend Micro,** questo tipo di truffa continuerà a tormentare le imprese nel 2023, con un **aumento previsto del 19,4%.**

Anche se l'uso di software per la sicurezza della posta elettronica può mitigare il rischio di BEC ed ostacolarne in qualche misura la crescita, questo tipo di attacco continuerà a rappresentare una tecnica criminale assai redditizia: si stima che **le perdite derivanti dagli attacchi BEC ammonteranno a circa 2,8 miliardi di dollari entro il 2027.**

BEC Gravità

Come conferma anche **l'Osservatorio Cyber realizzato da CRIF**, le attività degli hacker continuano con grande intensità.

Il numero **di account che hanno visto compromesse le proprie credenziali è significativamente aumentato nella prima metà del 2022,** in combinazione con altri dati utilizzati da hacker e frodatori. **In Italia** il numero di **alert relativi a dati rilevati sul dark web** è aumentato del **+44,1**% rispetto al semestre precedente.

BEC Gravità

Questi attacchi possono essere finanziariamente devastanti per le aziende, tanto che in un recente avviso il Federal Bureau of Investigation (FBI) avverte che la **BEC è una grave minaccia per l'economia globale.**

I tentativi di BEC sono maturati al punto che si parla di "BEC-as-a-service", una chiara indicazione del fatto che i criminali informatici stanno diventando abbastanza esperti di tecnologia da poter vendere i loro set di competenze. L'abbondanza e l'accessibilità delle informazioni online contribuisce inoltre in modo rilevante al fenomeno, agevolando gli aggressori nel perfezionare ulteriormente i loro schemi e a renderli ancora più mirati: la scarsa cura nell'impostare le proprie password può rendere facile il furto di credenziali, e **una grande quantità di dati di accesso è venduta sul dark web.**

BEC Gravita’

Questi attacchi possono essere finanziariamente devastanti per le aziende, tanto che in un recente avviso il Federal Bureau of Investigation (FBI) avverte che la **BEC è una grave minaccia per l’economia globale.**

I tentativi di BEC sono maturati al punto che si parla di “BEC-as-a-service”, una chiara indicazione del fatto che i criminali informatici stanno diventando abbastanza esperti di tecnologia da poter vendere i loro set di competenze. L’abbondanza e l’accessibilità delle informazioni online contribuisce inoltre in modo rilevante al fenomeno, agevolando gli aggressori nel perfezionare ulteriormente i loro schemi e a renderli ancora più mirati: la scarsa cura nell’impostare le proprie password può rendere facile il furto di credenziali, e **una grande quantità di dati di accesso è venduta sul dark web.**

BEC Gravità

Come conferma anche **l'Osservatorio Cyber realizzato da CRIF**, le attività degli hacker continuano con grande intensità.

Il numero **di account che hanno visto compromesse le proprie credenziali è significativamente aumentato nella prima metà del 2022,** in combinazione con altri dati utilizzati da hacker e frodatori. **In Italia** il numero di **alert relativi a dati rilevati sul dark web** è aumentato del **+44,1**% rispetto al semestre precedente.

BEC Fraud Tipologie

Gli attacchi di BEC tendono a rientrare in due categorie: su larga scala ed estremamente mirati.

La prima categoria è stata denominate “BEC-as-a-Service”: gli attacchi si basano su un meccanismo molto semplice in modo da poter raggiungere un numero più alto di vittime.

Gli attaccanti inviano messaggi semplificati in massa da account di posta gratuiti per attirare quante più vittime possibile. Di solito questi messaggi non sono particolarmente sofisticati ma sono molto efficienti.

Qualsiasi dipendente potrebbe essere una potenziale vittima. Ovviamente un messaggio di questo tipo contiene svariati campanelli d’allarme: non viene usato nessun account corporate e il mittente non è, evidentemente, madre lingua.

BEC Fraud Tipologie

Strategie più avanzate: attacchi BEC mirati.

Il procedimento :

per prima cosa gli attaccanti violano una casella di posta intermedia accedendovi abusivamente.

Successivamente, una volta trovata nella casella violata una corrispondenza «adatta» (ad esempio rapporti relativi a questioni finanziarie o problematiche tecniche connesse alle attività di lavoro), continuano la corrispondenza con la società presa di mira, impersonando l'azienda intermediaria.

Spesso l'obiettivo è quello di persuadere la vittima affinché invii del denaro o installi un malware.

Questa tipologia di attacco si è rivelata particolarmente efficace.

Non è una tecnica sfruttata solamente da "piccoli" criminali alla ricerca di facili guadagni.

BEC FRAUD

Reati generalmente ipotizzati:

Benché non preveda necessariamente la commissione di specifici crimini informatici, e sia comunque realizzato mediante strumenti telematici, questa frode prevede l'incriminazione per i reati previsti dagli Articoli 494 (sostituzione di persona) e 640 (truffa) del codice penale.

Il *modus operandi* si può così riassumere:

Ad un dirigente aziendale vengono inviate delle *email* create *ad hoc* così da apparire come provenienti da una figura aziendale ampiamente sovra ordinata rispetto a lui nell'organigramma societario;

Con le mail viene artatamente chiesta al dirigente la piena ma riservata collaborazione per l'avvio di operazioni finanziarie o di mercato in capo all'azienda per le quali è necessario movimentare ingenti fondi ;

Business Email Compromise (BEC)

Il Caso

Il direttore della delegazione di Confindustria presso l'Unione Europea a Bruxelles riceve un'e-mail dal suo superiore:

"Caro G., dovresti eseguire un bonifico di 500.000 euro su questo conto corrente. Non mi chiamare perché sono in riunione con il presidente e non posso parlare".
Mittente: M. P.

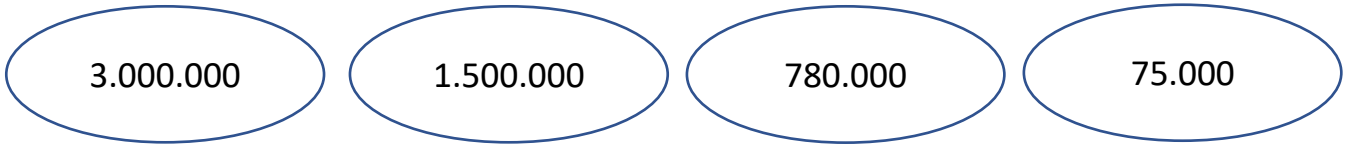
Il funzionario di Confindustria a Bruxelles ha eseguito il bonifico e 500.000 euro sono passati da un conto di Confindustria ad un conto estero di cui non si conosce l'intestatario.

Business Email Compromise (BEC)

La società calcistica S.S. Lazio, a marzo 2018 ha pagato l'ultima rata per il giocatore De Vrij su un conto bancario diverso da quello indicato dal club olandese del Feyenoord di Rotterdam. E così, due milioni di euro sono andati in fumo…

Un'azienda locale ha pagato 6.500.000 € (in tre tranche)

Un'altra 1.800.000 €, un'altra 500.000 €, un'altra 78.000 €, un'altra 42.000 € fino ad arrivare anche a solo 1.800 €



Business Email Compromise (BEC)

Gli attacchi tipo CEO Fraud e le BEC non contengono allegati, ma solo la parte testuale di un messaggio, nel quale l'attaccante cerca solo di rendersi credibile, "clonando" al meglio il mittente.

L'obiettivo è che la vittima riconosca il messaggio come veritiero, proveniente da una fonte certificata e autorevole. A quel punto, l'aggressore chiederà al suo bersaglio di compiere un gesto specifico, che sia un trasferimento di denaro o fornire l'accesso a informazioni riservate. Quest'ultimo non si insospettirà, perché il messaggio non contiene allegati (considerati pericolosi). Quindi probabilmente eseguirà la richiesta, soprattutto se operazioni simili (bonifici, ecc.) avvengono già in azienda con le stesse modalità.

Varianti della Business Email Compromise

Questa frode si sviluppa in svariate modalità:

Viene definita “The Man in the Mail” - “Bogus Invoice Scheme” - “Supplier Swindle” o “Invoice Modification Scheme”;

“CEO Fraud” o “Business Executive Scam”: una richiesta di bonifico bancario viene inviata dall’account compromesso di un dirigente aziendale di alto livello (CEO o Chief Financial Officer) a un dipendente all’interno dell’azienda, che è in genere responsabile dell’elaborazione di tali richieste. È la variante di phishing definita anche “whaling”, perché punta al “pesce grosso”;

Business Contacts through Compromised E-mail: al dipendente di un’azienda hanno violato la sua e-mail aziendale che viene utilizzata per comunicazioni personali e di lavoro. Le richieste di pagamenti di fatture a conti bancari controllati dai frodatori vengono inviate dall’e-mail di questo dipendente a più clienti acquirenti, identificati dall’elenco dei contatti;

Come difendersi dalla truffa BEC

- Usare credenziali di accesso alle mail robuste e sicure, quindi impostare una corretta gestione delle password;
- Non utilizzare in azienda indirizzi e-mail basati su webmail, perché sono facilmente accessibili ed attaccabili;
- Leggere le mail con attenzione, soprattutto quelle che si riferiscono a pagamenti. Nel dubbio non chiedere la conferma usando lo stesso indirizzo, perché ci risponderebbe il truffatore. Usare il telefono, o contattare direttamente il mittente utilizzando l'indirizzo presente nella rubrica aziendale oppure un altro indirizzo e-mail;
- Verificare il mittente delle e-mail: un dettaglio (anche solo una lettera!) potrebbe fare la differenza. Alcuni esempi di come è facile indurre in inganno con un indirizzo e-mail modificato ad arte: l'e-mail reale info@pippodomus.com potrebbe essere trasformata dal truffatore in: info@pippodornus.com o info@pipp0domus.com, info@pippo-domus.com;
- E soprattutto: evitare di pensare "figurati se una cosa del genere può succedere a me".

Può succedere a chiunque, se non si è attenti e consapevoli.

Varianti della Business Email Compromise

Business Executive and Attorney Impersonation: le vittime vengono contattate da truffatori che di solito si identificano come avvocati o rappresentanti di studi legali e sostengono di trattare questioni riservate o urgenti. Le vittime vengono spinte dal truffatore ad agire rapidamente o segretamente nella gestione del trasferimento di fondi. Questo tipo di truffa può verificarsi alla fine della giornata o della settimana lavorativa ed essere programmata per coincidere con la chiusura delle attività delle istituzioni finanziarie internazionali.

Data Theft (furto di dati): le richieste fraudolente vengono inviate utilizzando l'e-mail compromessa di un dirigente. I destinatari della richiesta sono figure dell'organizzazione aziendale che conoscono dati importanti, come risorse umane, contabilità o auditing. Queste richieste, in genere, si verificano prima di una richiesta fraudolenta di bonifico bancario.

Attacchi di BEC. Nuove frontiere

La nuova frontiera degli attacchi informatici sono le truffe alle email aziendali

Molte gang di ransomware potrebbero presto focalizzarsi sui cosiddetti attacchi Bec, più redditizi e decentralizzati

BEC Nuove frontiere

Lo scorso giugno, in una presentazione tenuta alla conferenza sulla Cybersecurity Rsa di San Francisco, il ricercatore esperto di truffe digitali Grane HASSOLD ha spiegato che un prossimo passo logico per le gang di Ransomware potrebbe essere quello di convertire le loro attività nei cosiddetti attacchi BEC **nel momento in cui il Ransomware dovesse diventare meno redditizio o comportasse un rischio maggiore per gli aggressori**

BEC Nuove frontiere

Negli USA l'FBI ha ripetutamente sottolineato che il denaro rubato attraverso le truffe BEC supera di gran lunga quello sottratto con gli attacchi di Ransomware anche se questi ultimi possono ottenere maggiore visibilità e causare danni perdite ingenti

Il Ransomware è però oggetto di grande attenzione e i governi di tutto il mondo stanno intervenendo per bloccarlo per cui alla fine il ritorno sull'investimento ne risentirà, sostiene HASSTOLD.

E' quindi probabile che emerga una nuova minaccia in cui gli attori più evoluti dietro le campagna di Ransomware **si sposteranno nel più redditizio e sicuro campo degli attacchi BEC**

BEC Nuove frontiere

Il Ransomware è oggetto di grande attenzione e i governi di tutto il mondo stanno intervenendo per bloccarlo per cui alla fine il ritorno sull'investimento ne risentirà, sostiene HASSTOLD.

E' quindi probabile che emerga una nuova minaccia in cui gli attori più evoluti dietro le campagna di Ransomware **si sposteranno nel più redditizio e sicuro campo degli attacchi BEC**

BEC Nuove frontiere

Storicamente gli attacchi BEC, che in molti casi hanno origine nei paesi dell'Africa Occidentale e sopratutto in Nigeria, sono meno evoluti dal punto di vista tecnico e fanno maggiore affidamento sulla ingegneria sociale.

HASSTOLD però sottolinea che molti malware assemblati per attacchi di Ransomware sono progettati per essere flessibili e modulari in modo che i cybercriminali possano riassemblare gli strumenti di cui hanno bisogno per altre specifiche truffe

BEC Nuovi scenari

La riscossione del denaro e le possibili evoluzioni.
Il cambio di campo
La crisi dei pagamenti in criptovalute
Il ritorno ai Money mules?

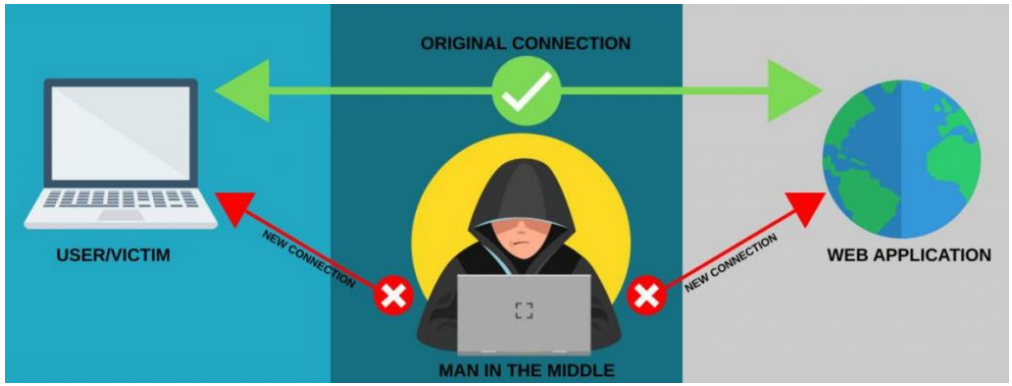
MAN IN THE MIDDLE
MAN IN THE MAIL , CEO FRAUD

Sostanzialmente fasi «tecnologiche» :

- Illecita intromissione negli account di posta elettronica o altri account della vittima per inserirsi in trattative commerciali e dirottare grossi importi dovuti a saldo di acquisti o cessioni

- illecita presa in gestione del cd «*client di posta*» della vittima

… e quindi «*social engineering*» …..



Man in the middle

Attacco man in the middle

(spesso abbreviato in MITM, MIM, MIM attack o MITMA, in italiano *"uomo nel mezzo"*) è una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro

MITM

- Ad esempio un attacco man in the middle è l'eavesdropping, in cui l'attaccante crea connessioni indipendenti con le vittime e ritrasmette i messaggi del mittente facendo credere loro che stiano comunicando direttamente tramite una connessione privata, con l'intera conversazione che è controllata invece dal malintenzionato in grado di intercettare tutti i messaggi importanti e/o iniettarne di nuovi. In molte circostanze questo è semplice, per esempio, un attaccante all'interno di un WI-FI access point non criptato, può inserire se stesso come *"uomo nel mezzo"*[2]. Altro tipo di attacco man in the middle è lo spoofing

Man in the middle ed evocazioni storiche

- Le ragioni della triste fine di Maria Stuarda
- Un classico esempio di intromissione nelle comunicazioni tra soggetti dopo averne violato i codici di segretezza
- Comunicazioni non solo violate ma anche alterate

MITM

- L'attacco può funzionare solo se nessuna delle due parti è in grado di sapere che il collegamento che li unisce reciprocamente è stato effettivamente compromesso da una terza parte, cosa di cui potrebbero venire a conoscenza comunicando con un canale diverso non compromesso. La maggior parte dei protocolli di crittografia includono una qualche forma di autenticazione endpoint specificamente per prevenire attacchi MITM. Ad esempio, TLS può autenticare una o entrambe le parti utilizzando una Certificate authority reciprocamente attendibile

Il criminale prima carpisce informazioni sulle aziende attraverso la rete internet, la *social engineering*, *insiders* aziendali, violando indirizzi e-mail, accedendo a *devices* aziendali smarriti o rubati, ecc., ma anche semplicemente (ma non solo) tramite visure C.C.I.A.A.
Successivamente, approfittando di diversi fattori contingenti quali giorni di chiusura, diverso fuso orario, ubicazione territoriale, lingue straniere che rendono difficoltosi sia i contatti in tempo reale come quelli telefonici (le aziende cinesi, ad esempio, si relazionano con quelle italiane esclusivamente a mezzo email), l'attaccante si sostituisce all'azienda *x* e si presenta alla ditta *y*.

Effettua poi ordinativi fraudolenti o finge di effettuare forniture attraverso pagamenti anticipati, oppure, nel caso di aziende con pregressi rapporti commerciali, comunica nuove coordinate bancarie per la ricezione di pagamenti di precedenti commesse ancora insolute.

Le false comunicazioni sono realizzate anche avvalendosi di indirizzi *email* appositamente creati che ricordano direttamente quelli dell'azienda presa di mira.

(esempio: se l'indirizzo reale della società XYZ S.p.A. è info@societaXYZ.com, il criminale creerà l'indirizzo societaXYZ@gmail.com oppure, se l'indirizzo del direttore commerciale è antonio.rossi@societaXYZ.com, verrà creato antonio.rossi@yahoo.com.)

La prima *email* di comunicazione del cambio dei recapiti aziendali con quelli utilizzati per la frode avviene proprio attraverso l'indirizzo *email* reale dell'azienda violata, che viene utilizzato *una tantum* dal reo per rendere più credibile la truffa.

FONTI NORMATIVE

Art. 615 ter C.P. Accesso abusivo ad un sistema informatico o telematico *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

Art. 617 sexies C.P. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso, con la reclusione da uno a quattro anni.*

Art. 494 C.P. Sostituzione di persona *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sè o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno.*

Art. 640 ter C.P. Truffa *Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.*

Man in the middle

Alcuni esempi concreti

Caso “ regna” mascherato in “regan”

Importo 2.500.000 $

Caso “fluid” mascherato in “fliud”

Importo 140.000 Euro

Man in the Browser (MITB)
Una frode finanziaria tecnologicamente avanzata

MITB è una sottospecie del più ampio fenomeno del Man in The Middle

In sostanza l'hacker si interpone tra due entità : il client (l'utente) ed un server o un router riuscendo non solo ad intercettare i messaggi inviati e ricevuti (sniffing), ma anche a modificarli (tampering)

MITB
Origini

MITB è da ascriversi al malware Zeus Trojan, conosciuto anche come Zbots, scoperto nel 2007 e diffusosi nel 2009-10 al fine di sottrarre dati finanziari.

Successivamente debellato dalle autorità USA è stato poi rieditato in altre forme similari a causa della messa in rete dei codici sorgente disposta incautamente dalle stesse autorità

MITB Diffusione

Principali tipologie di diffusione :

- messaggi spam via email;
- drive by download tramite una applicazione dannosa;
- keylogger;
- compilazione di un form.

MITB modalità operative

In ambito bancario viene descritto come l'interposizione fra il sistema centrale dell'intermediario (banca) e quello del singolo (cliente).

Annidatosi in un notevole numero di computer li trasforma in una vera e propria botnet.

Dotato di sofisticate capacità di elusione dei migliori antivirus si annida silente nel pc della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente.

MITB modalità operative

Il malware resta completamente in silenzio attivandosi solo nel momento in cui l'utente si collega a un sito finanziario compreso fra quelli che il programma ha posto nel **mirino (targeted banks).**

Solo allora il malware si risveglia captando il collegamento dell'utente e propinandogli una pagina/video esattamente identica a quella del suo solito ed abituale intermediario bancario.

MITB modalità operative

Unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente :

La stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (cd protocollo di trasferimento ipertestuale, Hyper Text Transfer Protocol) «http» e non «https» (Hyper Text Transfer Protocol Secure).

MITB modalità operative

Indotto a ritenersi nel normale e sicuro ambiente di connessione l'utente è a tal punto completamente in balia dei criminali.

Il malware infatti attiva una prima finestra a modulo, sempre apparentemente riferita alla banca dell'utente che gli richiede conferme di sicurezza con invito a compilare campi del modulo con le proprie credenziali ed il codice OPT generato dal token, procedure di sicurezza ulteriori che le banche attivano talvolta in caso di connessioni ai servizi bancari on line da indirizzi IP diversi da quelli abituali dell'utente.

MITB modalità operative

Il tutto rafforza il convincimento della piena regolarità della situazione da parte del cliente il quale compila i campi del modulo fittizio «consegnando» tutte le sue credenziali al criminale.

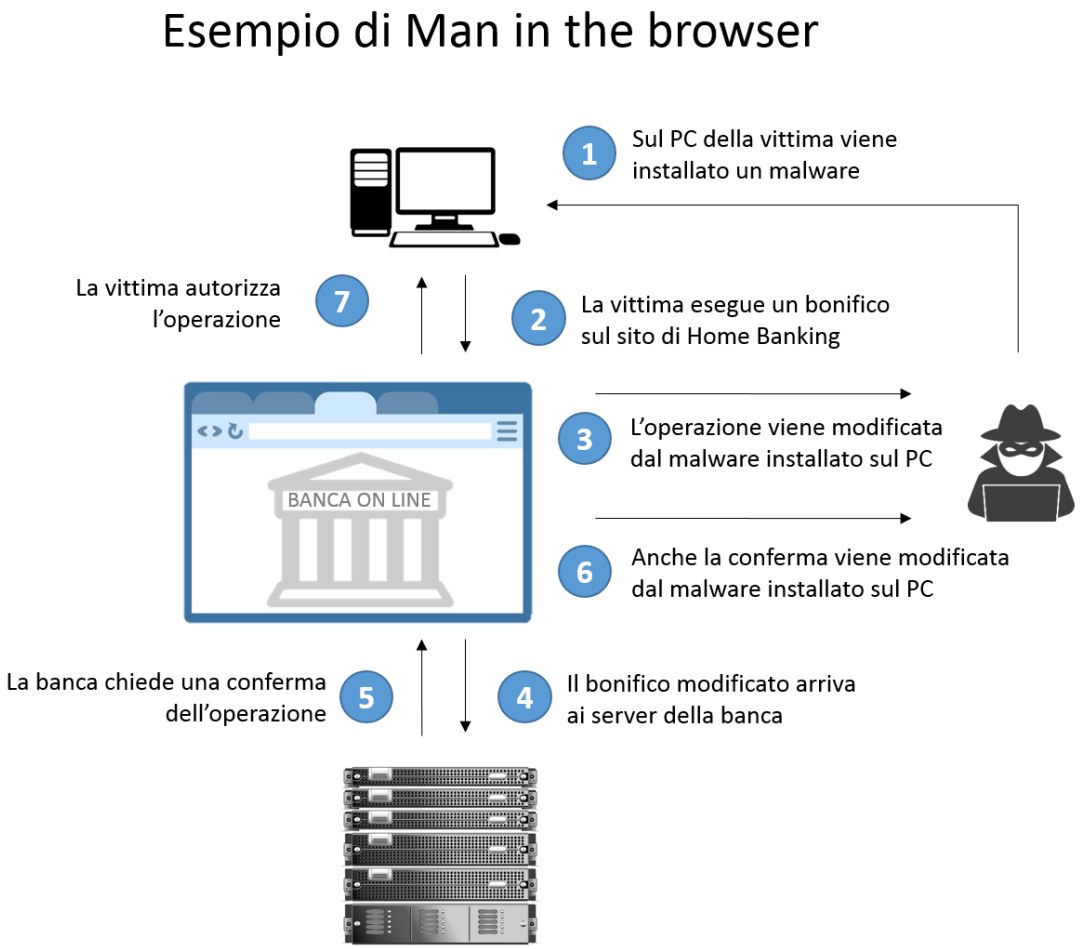
Quest'ultimo attua così la *captatio* dei codici di autenticazione utilizzandoli in tempo reale.

Nel contempo l'utente viene ulteriormente ingannato da un messaggio di attesa che dopo pochi minuti si conclude con l'impossibilità di procedere all'operazione e ritentare più tardi-

MITB modalità operative

Come nei più collaudati schemi del phishing bancario l’hacker accede ai servizi on line del cliente (ancora) ignaro della truffa disponendo urgenti operazioni di pagamento a terzi complici che adotteranno a loro volta altre strategie per celare i successivi dirottamenti dei capitali sottratti.

MITB Esempio



Man In the Browser
Esempio

Il Man in the Browser è un attacco che ha colpito principalmente istituzioni finanziarie.

Eccone le fasi di un esempio tipico

MITB Esempio Fase 1

Ipotizzando che un correntista della banca X chiedesse di eseguire un bonifico on line il suo client potrebbe eseguire una request HTTP POST contenente, come body della chiamata, un JSON (semplificato) di questo tipo:

{"ndg": 87654321, "order": "Cliente Vittima",

"amount": 1234.56,
"cur": "EUR",
"iban-payee": "IT31K0558401650000000000001", "payee": "Luigi Luzzatti”}

MITB Esempio Fase 2

Prima di eseguire la chiamata al server e anzi, prima ancora di crittografare il contenuto della chiamata HTTPS, il trojan potrebbe intervenire modificando il JSON con:

{ "ndg": 87654321,

"order": "Cliente Vittima",

"amount": 1234.56,

"cur": "EUR",

"iban-payee": "IT98M0504003200453242374232",

"payee": "John Robber" }

Questo consentirebbe ad un attaccante di dirottare la somma di 1.234,56 EUR da:

Luigi Luzzatti

IBAN IT31K0558401650000000000001

a John Robber

IBAN IT98M0504003200453242374232

MITB Esempio Fase 3

L'attacco potrebbe non fermarsi a questa modifica. Quando poi il server processa la richiesta del client, la banca potrebbe chiedere una conferma dell'operazione, che però verrebbe mostrata sul browser infetto. E così, a fronte di una response HTML tipo:

```
<p>Confermi l'invio di un bonifico di <b>1.234,56 EUR</b> a:</p>
<p>
<b>John Robber</b> (IBAN: IT98M0504003200453242374232)?
</p>
```

MITB Esempio Fase 4

Il trojan potrebbe intervenire nuovamente e modificare il codice riportando i valori iniziali richiesti dalla vittima:

Confermi l'invio di un bonifico di 1.234,56 EUR a:

Luigi Luzzatti (IBAN: IT31K0558401650000000000001)?

A questo punto, la vittima dell'attacco **Man in the browser** accetterebbe l'operazione e l'aggressione avrebbe successo. 1.234,56 EUR sono stati trasferiti a John Robber.

MITB Difese

Ardue le strategie di difesa

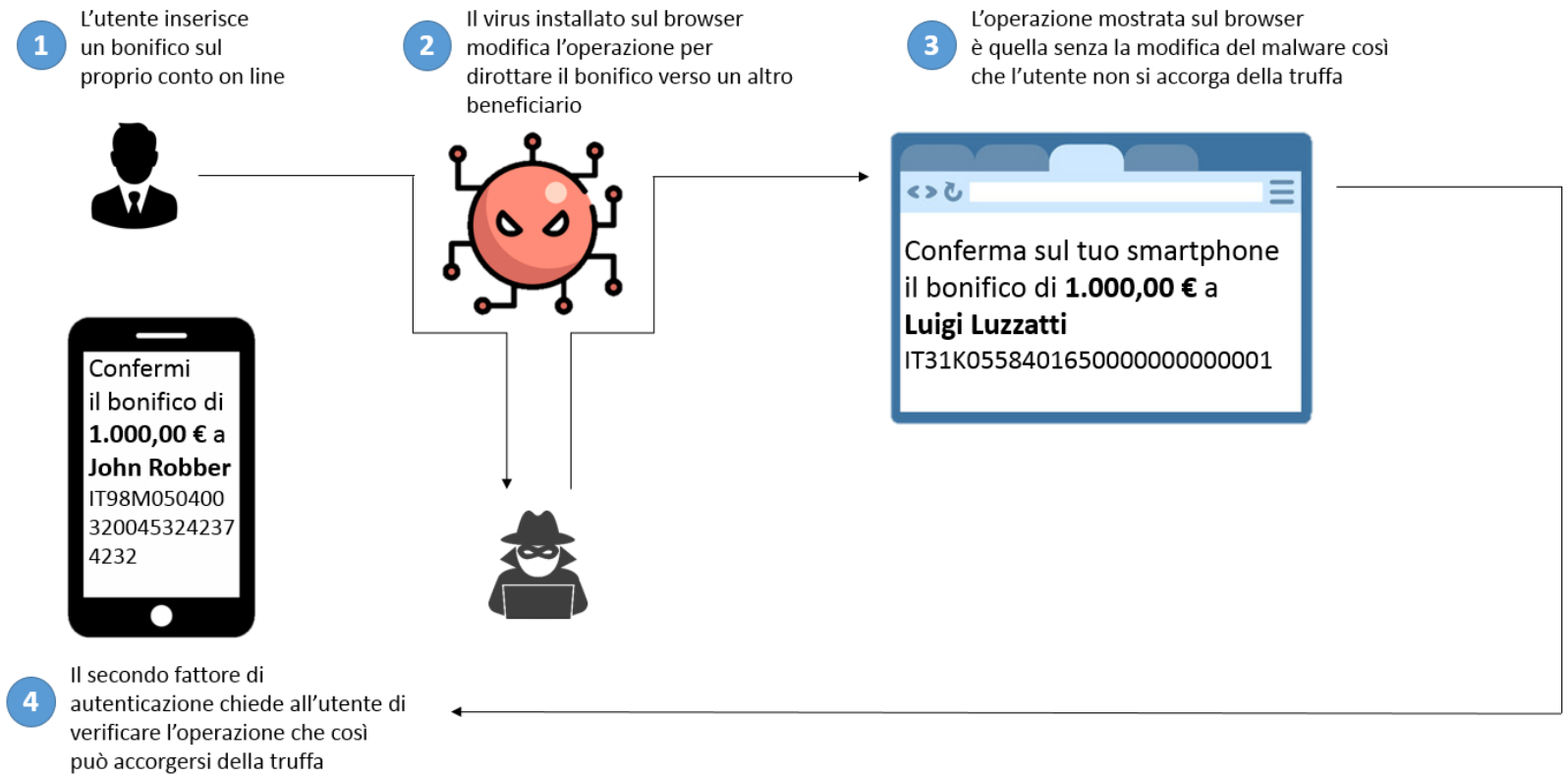
il trojan interviene prima (per le request) e dopo (per le response) che il browser cripti e decripti il traffico in arrivo tra client e server

Strumenti di difesa

Lato utente, come sempre, è indispensabile tenere aggiornato il sistema operativo e il browser alle ultime versioni possibili.

Oltre a dotarsi di un buon antivirus per intercettare eventuali infezioni da parte di questi trojan.

Tentativo di mitigazione contro il Man in the browser



MITB Strategie di difesa

Sniffing dei dati

L'applicazione Web ha poche difese contro il **Man in the browser** in caso di *sniffing*, ovvero l'intercettazione dei dati senza alcuna modifica,

L'applicazione può intervenire solo ex post quando il malintenzionato proverà ad effettuare lui stesso la login, potranno attivarsi i sistemi di controllo (accesso anomalo da device mai utilizzato, da un'area geografica nuova, ecc.).

Sniffing

Ma i dati rubati potranno essere utilizzati anche in maniera differente, come nel Credential Stuffing

Lo sniffing dei dati può riguardare, a titolo esemplificativo e non esaustivo:

Furto delle credenziali di accesso

Furto del cookie di sessione (Session Hijacking)

Furto di informazioni riservate quali:

- numero di carta di credito
- codici di autorizzazione
- altri dati finanziari

Tampering dei dati

Più complicato è il *tampering*, ovvero la modifica, delle informazioni passate tra client e server (come nell'esempio di Man in the browser visto precedentemente).

Il server infatti, si vedrebbe arrivare una richiesta da un device già utilizzato (e magari certificato dall'utente), con la solita geolocalizzazione e lo stesso operatore di rete.

E per questo è difficile, per il layer dell'applicazione Web che risiede sul server, distinguere un'operazione corretta da una modificata.

Secondo fattore di autenticazione

Una forte difesa contro l'attacco **Man in the browser** può essere la presenza di un secondo fattore di autenticazione che non risieda nel browser, così da poter validare l'operazione in un canale che non è stato infettato (*out of band communication*).

Per esempio, nell'attacco visto prima, una volta eseguita l'operazione, la banca avrebbe potuto chiedere una conferma sullo smartphone del cliente indicando chiaramente:

- Importo
- Beneficiario
- IBAN beneficiario

Dubbi sul secondo fattore di autenticazione

La presenza del secondo fattore di autenticazione su un canale *out of band* è valido solo se:
L'utente legge e verifica prima di autorizzare
Lo smartphone non è anch'esso infettato
.

Secondo fattore I dubbi

- I dubbi (sollevati da alcuni) sul primo punto sussistono soprattutto perché in questo contesto, il secondo fattore di autenticazione verrebbe utilizzato per scaricare sull'utente l'onere della verifica per una possibile falla presente nella catena di erogazione dell'applicazione Web. Quindi il secondo fattore non completerebbe solo la fase di autenticazione, ma richiederebbe all'utente un controllo su ciò che è stato inserito in quanto sussiste la possibilità che il canale non sia sicuro. Il tutto potrebbe far venire meno il senso di fiducia di chi utilizza i servizi on line

MITB Contromisure di massima

- mantenere costantemente aggiornato il browser e controllare periodicamente plug-in, add-on o estensioni installate;

- adottare un browser specifico da usare esclusivamente per connessioni particolari (ad esempio per eseguire operazioni finanziarie on line);

- utilizzare autenticazioni a due fattori;

-eseguire analisi comportamentali (ovviamente lato server banca) che possano evidenziare comportamenti anomali lato cliente

MITB Evoluzioni

Riconducibili originariamente alla installazione delle cd “librerie” o di “assistenti di navigazione” noti come Browser Helpers Object (BHO).

Recentemente fanno oramai ampia leva su strategie di social engineering e di “blowlocking” (blocco del servizio inducendo l’utente a installare nuove versioni di applicazioni con contenuti malevoli)

MITB

Il complesso regime delle responsabilità.

Norma cardine il D.Lgs. 218.2017, in attuazione di Direttiva 2015/2366/UE, operativa dal 14.9.2019. :

MITB il regime delle responsabilità

Si dispone che (art.10 comma 1)

«qualora l'utente dei servizi di pagamento (cliente) neghi di aver autorizzato un'operazione di pagamento,

è onere del prestatore di servizi (intermediario/banca) provare che l'avvenuta operazione di pagamento

MITB il regime delle responsabilità

- è stata autenticata;
- è stata correttamente registrata e contabilizzata;
- e che non ha subito il malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti

MITB il regime delle responsabilità

Tale prova non è pero sufficiente essendo previsto infatti dal successivo comma 2 del medesimo articolo

«l'onere dell'intermediario (di) fornire la prova della frode, del dolo o della colpa grave in capo all'utente»

In caso di mancato assolvimento dell'onere probatorio l'intermediario è tenuto a riaccreditare immediatamente l'importo sottratto sul conto del cliente

MITB il regime delle responsabilità

La responsabilità dell'utente resta quindi circoscritta a casi di suo comportamento fraudolento o di inadempimento doloso o gravemente colposo dei seguenti obblighi contrattuali:

1) utilizzo dello strumento di pagamento in conformità delle condizioni prefissate;

2) tempestiva denuncia di furto, smarrimento.

MITB il regime delle responsabilità

In sostanza un regime di speciale protezione e **favor probatorio a beneficio degli utenti frutto di una netta scelta legislativa** di far gravare l'onere probatorio sul prestatore dei servizi di pagamento **(banca)** ispirata alla logica che costui/ei è il **soggetto meglio in grado di gestire il rischio** facendo ricadere il danno dell'uso fraudolento sulla massa degli utenti mediante la sua parcellizzazione

MITB il regime delle responsabilità

Una disciplina di responsabilità chiaramente ispirata al **principio del «rischio di impresa»** per cui è razionale far gravare sull'impresa i rischi statisticamente prevedibili legati ad attività oggettivamente pericolose che riguardano una moltitudine di consumatori e utenti

Il tutto nel presupposto che l'impresa, potendo determinare il regime dei prezzi per i beni o servizi offerti, può in sostanza spalmare sulla moltitudine degli utilizzatori il rischio di impieghi fraudolenti dei mezzi di pagamento evitando che quel rischio gravi in capo al singolo utente

Man in the browser e phishing

Differenze nelle tecniche criminali e nei regimi di responsabilità

L’importante decisione (n.3857/2013) del Collegio di Coordinamento dell’Arbitro Bancario Finanziario (ABF) di Milano

.

MITB e Phishing

Phishing : l’inganno dell’utente e l’aggiramento dei presidi informatici di sicurezza avvengono attraverso metodi ormai più che noti (mail o sms civetta, false comunicazioni via telefono) che il cliente mediamente diligente è oggettivamente in grado di schivare

MITB e Phishing

L’utente in sostanza è vittima di una «colpevole credulità» in quanto **comunica le proprie credenziali di autenticazione al di fuori del circuito operativo dell’intermediario** abboccando a forme di truffa ormai ben note anche ai non esperti della materia non tenendo conto anche delle continue campagne preventive degli istituti bancari in tema di cybercrime. Spesso del resto le mail trappola usano un linguaggio maccheronico o con errori nel lessico o nel logo della banca.

MITB e Phishing

MITB Il meccanismo di appropriazione indebita dei codici di sicurezza personali dell’utente è più subdolo e in grado di sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio

MITB e Phishing

Nell MITB il subdolo congegno di infezione si attua attraverso «un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino»

MITB e Phishing

L’unica differenza consta nell’acronimo del protocollo di trasferimento individuato come un normale http e non già come un https protetto.

Questa variazione compare solo nella stringa di intestazione della video-schermata mescolata ad almeno cinquanta sessanta caratteri, barre e altri segni di punteggiatura informatica.

Tale differenza sfugge normalmente all’attenzione di chiunque si accosti ad una pagina della rete e più che mai sfugge a chi si accosti alla pagina di un sito bancario per compiere una operazione

MITB

In sintesi nella richiamata decisione del Collegio che delinea una ipotesi di vera e propria **«probatio diabolica»** a carico dell'intermediario bancario è da escludersi ogni qualsivoglia tipo di colpa anche lieve dell'utente vittima della frode purchè abbia utilizzato lo strumento di pagamento conformemente agli accordi contrattuali e abbia fatto tempestiva denuncia della frode alle Autorità preposte e alla banca