BEC Fraud Losses Grew to $1.3 Billion in 2018: FBI

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CVr6vXRk–E/bec-fraud-losses-grew-13-billion-2018-fbi

---

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

Seduto al tavolino di un bar accanto gli uffici di **Italiaonline** ad Assago, un hacker ha rubato credenziali di accesso alle caselle di posta elettronica di 1 milione e 400.000 clienti dei servizi di **Libero Mail** e di **Virgilio Mail.**

Sono questi gli esiti della vicenda raccontata dal *Corriere della Sera dell'attacco hacker avvenuto nel milanese,* messo a punto da un hacker 24enne.

Il criminale informatico, secondo la ricostruzione del Corriere, sarebbe entrato nelle rete Wifi dell'azienda attraverso l'uso di un computer portatile e di una grande antenna, usando la password di un dipendente e avrebbe iniziato l'attacco, riuscendo a violare **1 milione e 400mila dati.**

Sulla vicenda, secondo il quotidiano, sta indagando la **Procura di Milano** e sta svolgendo una apposita ispezione il **Garante per la privacy,** avvisato del Data Breach da Italiaonline come

impone il GDPR, il nuovo regolamento europeo.



L'azienda ha fatto sapere che il sistema antintrusione ha funzionato dichiarando che "*allo stato attuale, non ci sono utenti che abbiano segnalato accessi indesiderati alla propria posta*".

Il rischio, invece, si palesa per chi usa la stessa password della posta elettronica per accede ad altre piattaforme, quali conti bancari: in questo caso è necessario cambiare immediatamente tutte le parole chiave, per evitare che i pirati informatici si introducano nella piattaforma bancaria.

Consigli sulle password

Avere password differenti per ogni account, email o conti correnti è una buona regola per non essere vittime di criminali informatici e dover fare i conti con furti di dati. E allora ecco qualche semplice consiglio su come ricordare password complesse, in modo da poter ricordare tutte le password più importanti.

1. Creare una "static string" (quella parte di password che resta sempre uguale)

1. Pensare ad una frase, al testo di una canzone, alle

citazioni di un film, ad una filastrocca o a qualcosa di simile, che sia facile da ricordare;
2. Prendere la prima lettera delle prime tre o prime cinque parole;
3. Aggiungere, tra una lettera e l'altra, un carattere speciale (ad esempio: #, @, / e simili).
4. Da questo momento in poi, è possibile basare tutte le proprie password uniche su questa singola stringa di caratteri.

2. Sfruttare la potenza dell'associazione di idee

1. In caso di necessità di una password per uno degli account online in uso (ad esempio per Facebook, Twitter, eBay, per l'online banking, per lo shopping online o i siti di videogiochi…), si deve prendere nota della prima parola che si associa ad un determinato sito o ad una certa piattaforma.
2. Ad esempio, se si sta creando una password per l'account di Facebook, si potrebbe associare al social media il colore blu, presente nel logo. Basterebbe, quindi, aggiungere la parola "blu", magari in lettere maiuscole, alla fine della "static string" creata in precedenza

Data breach, hacker 24enne ruba accessi di 1,4 milioni di email

---

Kaspersky Links ShadowHammer

Supply-Chain Attack to ShadowPad Hackers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/pn0ypAdfpOo/kaspersky-links-shadowhammer-supply-chain-attack-shadowpad-hackers

---

Source Code of Iran-Linked Hacking Tools Posted Online

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Xz-NmgF2EV8/source-code-iran-linked-hacking-tools-posted-online

---

WannaCry ‘Hero’ Marcus Hutchins Pleads Guilty to Creating Malware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Ex9g8eLqUTE/wannacry-hero-marcus-hutchins-pleads-guilty-creating-malware

Cybercrime, cosa si vende nel dark web?

Cosa succede quando la parte di nascosta del web, dove hanno luogo le transazioni più sregolate decide di rinfrescare la sua impostazione commerciale?

Le implicazioni per la cybersecurity sono sicuramente molte, un tempo il **Dark web**, per definizione, era un luogo dove la sola parola garanzia era impronunciabile: le transazioni avvenivano in un contesto di massima insicurezza, senza alcuna certezza. Oggi, mimando il successo dell'on-line retail il Dark web si è dotato di uno dei componenti chiave del successo della sua controparte legale, le garanzie. Non solo, queste piattaforme distorte di eCommerce operano su piattaforme che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto, il tutto incorniciato con un'interfaccia intuitiva e responsive facilmente navigabile. Non mancano neppure elementi di customer care come FAQ, chat di supporto e dettagliate pagine di aiuto.

La valuta principale di scambio non è il dollaro e neppure lo yen, qui la fanno da padrone le cripto valute grazie alle loro caratteristiche che permettono grande anonimato e scarsa tracciabilità.

Tra la merce a disposizione al primo posto per numero di inserzioni regnano ancora gli stupefacenti, ma a breve distanza troviamo innumerevoli *hacking tools* e pacchetti di dati sensibili illegalmente ottenuti. Siamo dinnanzi a una *regolarizzazione* della delinquenza e le implicazioni per la cybersecurity sono molte.



Cybercrime commodity: i must have

Ma quali sono i programmi più popolari in vendita all'interno di queste piattaforme? Alcuni esempi delle categorie più popolari:

Tra i vari malware offerti sulle piattaforme, i più pericolosi sono sicuramente i Remove Access Trojan. Questa variante di software dannoso può mettere in condizione il pirata informatico di prendere totalmente il controllo del pc della sua vittima. Questo la rende scoperta e vulnerabile nei confronti di una pletora di potenziali crimini: dal furto di dati sensibili – dalle carte di credito, Paypal, dati di homebanking – al vero e proprio furto d'identità, ma i RAT sono anche usati per accedere alle webcam integrate che vengono sfruttate a fini di ricatto. Attenzione però, non sono solo i personal computer a essere aperti al rischio di questa infezione, alcune varianti di malware sono state in grado di contagiare anche nei dispositivi mobile che utilizzano l'OS Android.

Anche in questo caso fioriscono le offerte di programmi più o meno differenti. I target più frequenti di questi programmi, utilizzati per sottrarre password, sono i siti social e di svago come Facebook e Spotify.

Il **phishing** è sicuramente uno dei vettori di cyberattacco più

diffusi, quindi non c'è da stupirsi se all'interno del Dark web esistono centinaia di inserzioni in vendita per pagine che in maniera camaleontica replicano siti di brand affermati come Netflix, Facebook, Twitter…

Oltre ai metodi già citati sono disponibili una pletora di opzioni di Hacking in vendita a prezzi inferiori ai 10 dollari: i keyloggers – software in grado di catturare tutto ciò che viene digitato sulla tastiera del PC -, vari software in grado violare reti Wifi e connessione Bluetooth e malware progettati per sottare Bitcoin.

Così come il mercato delle tecnologie IT ha sviluppato offerte in grado di soddisfare l'utente finale secondo tutte le sue necessità allo stesso modo anche il Dark Web ha sviluppato pacchetti omnicomprensivi per aspiranti truffatori. In particolare, questo è stato osservato nel mercato della falsificazione di documenti ufficiali. Sono stati creati veri e propri template Photoshop – completi di dettagliate istruzioni per l'uso – che coprono tutto il ventaglio dei documenti: carte d'identità, patenti, passaporti, bollette, fatture… Questi template sono usati in combinazione con i cosiddetti "Fullz", termine proprio dello slang degli hacker, che indica il pacchetto completo dei dettagli personali (nome, codice fiscale, data di nascita, numero di conto corrente bancario…) sottratti alla vittima di furto d'informazioni e ugualmente disponibili sul Dark web. Il risultato dell'unione di questi dati con i template (venduto appunto come soluzione completa) viene usato principalmente per commettere frodi bancarie. Ciò, in breve, è significativo di quanto si sia evoluto questo mercato "underground": il criminale intenzionato a commettere una frode può effettivamente acquisire un pacchetto completo di strumenti e istruzioni per l'uso atte a questa attività criminale.

Cybercrime commodity: un epidemia in procinto?

Quelli elencati non sono altro che alcuni semplici esempi dell'enorme business che è il cybercrime oggi. Di certo è un'utopia l'augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono portare significativi benefici atti a scongiurare questi attacchi e mantenere la propria sicurezza. Un consiglio è quello di utilizzare, laddove possibile, un sistema autenticazione a due fattori, che assicura un'ulteriore barriera di protezione anche nel caso in cui venga sottratta la password. Un altro facile accorgimento riguarda l'igiene delle password: una sicura non deve essere scontata, non deve richiamare al tuo nome/data di nascita o a quello dei tuoi cari, non deve essere eccessivamente corta e deve includere caratteri speciali. Il cambio di paradigma necessario per assicurarsi maggiore protezione non è solo tecnico, ma anche culturale: lo sforzo combinato deve avere luogo lungo tutta la filiera digitale per educare ed educarsi sull'importanza della sicurezza online è la vera strada per rendere inefficaci, se non solo per gli hacker più esperti, tutti gli strumenti che pullulano sulle piattaforme presenti nel Dark web.

La battaglia deve essere combattuta su due fronti: tecnico e culturale. Si è reso imperativo l'acquisto di skill, anche basilari, per affrontare le criticità della cybersecurity. Una buona strada per raggiungere questo obiettivo è quella di intraprendere corsi di formazione. Il mercato ha, fortunatamente risposto a questa necessità ed è oggi possibile prendere parte a corsi tailor made per ogni tipo di livello richiesto, dalle basi di Cybersecurity awareness a sessioni su argomenti più avanzati come l'Ethical Hacking.

Sul lato più "company", uno dei migliori metodi, per business e provider di servizi web, di comprendere a quali rischi

possono essere soggetti i propri domini, app, etc… è quello di eseguire un Vulnerability Assessment test: si tratta di un’analisi di sicurezza effettuata per identificare tutte le vulnerabilità potenziali di sistemi, pagine web, network e applicazioni. Come fare per effettuarne uno? Sono disponibili molti strumenti automatizzati.

Questi tools effettuano controlli approfonditi su ogni sistema o applicazione e riconoscono le vulnerabilità presenti. Un altro aspetto importante da considerare è la velocità di scansione. La celerità di questi tool rende possibile la scansione di un perimetro molto ampio in un periodo di tempo relativamente breve, fornendo, inoltre, un buon livello di dettaglio, questo per garantire la massima efficienza nell’intervenire e correggere eventuali falle di cybersecurity presenti nel sistema.

https://www.key4biz.it/cybercrime-cosa-si-vende-nel-dark-web/255313/

Operator of Codeshop Cybercrime Marketplace Sentenced to Prison

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/6PA-hMsIVWk/operator-codeshop-cybercrime-marketplace-sentenced-prison

---

Cybercrime, quali sono le tecniche d'attacco alla luce del Clusit 2019

Nello scorso anno il 95% dei cyberattacks è durato meno di 3 ore, ma di essi il 2% si è protratto oltre le 24 ore consecutive, come riportato dal Rapporto **Clusit** 2019.

Importante allora è la **Cyber resilience**, cioè la "*capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso*", spesso nelle situazioni di **Zero-day attach** cioè un "*attacco compiuto sfruttando vulnerabilità non ancora note/risolte*".

Altro dato importante è valorizzare e comprendere la COMPONENTE UMANA (come accade nei malware dove il maggior impatto è dato dal*Man-in-the-browser*).

Ancora, molto sviluppata è la **Social engineering** che è la "*tecnica di attacco basata sulla raccolta di informazioni mediante studio/interazione con una persona*".



Infatti la "***User Behavior Analytics (UBA)*** *o analisi comportamentale dell'utente, aggiunge un ulteriore elemento per il calcolo del valore di rischio della singola*

transazione, e mira ad individuare prontamente le azioni dei cyber criminali che cercano di impersonificare la vittima, autenticandosi con le sue credenziali. Lo fa analizzando una grande quantità di dati e informazioni sul comportamento online dell'utente, generati dai sistemi e dalla rete, e finora ignorati. Questi elementi, disponibili già oggi, consentono di aggiungere contesto all'utente e al dispositivo usato nella transazione, e contribuire a misurare in maniera accurata il livello di rischio di ciascuna operazione".

Compartecipazione della vittima

L'elemento che ha contribuito al successo delle principali campagne di malware dell'anno è stata la compartecipazione della vittima, che spesso ha aperto ed eseguito gli allegati malevoli ricevuti via mail. Questo nella noncuranza delle più elementari norme di precauzione, e dei messaggi di avvertimento generati dalle versioni più recenti dei prodotti di produttività, come Office.

Il fenomeno è più grave di quanto si possa immaginare. All'atto pratico, non solo la vittima ha aperto per curiosità una mail che nella maggior parte dei casi non attendeva, ma si è anche fidato delle informazioni fallaci che ha visto a schermo, ed ha collaborato attivamente con l'attaccante abilitando l'esecuzione delle macro all'interno dei documenti o dei file.

Anno nuovo, modus operandi nuovo (webinject)

Una nuova tattica è emersa nella seconda parte del 2018. In almeno due campagne studiate da **IBM Security,** i malware sono stati usati per seguire e osservare le attività online della vittima senza alcun intervento, lasciandogli effettuare il login e la navigazione all'interno del sito bancario,

intervenendo però con webinject al momento dell'effettiva operazione dispositiva, sostituendo le coordinate bancarie del beneficiario.

I webinject permettono di alterare ciò che viene visualizzato all'interno del browser. In questo modus operandi i **webinject** mostrano a video le coordinate bancarie del destinatario, ma all'invio della transazione passano al sito bancario altre coordinate bancarie. La frode diventa trasparente nei confronti della banca, e difficile da individuare per l'utente non attento. La vittima inserisce anche il secondo fattore di autenticazione (solitamente inviato via SMS), e riceve poi segnalazione della avvenuta transazione con l'importo effettivamente immesso, che vede tra le operazioni effettuate. Quello che un occhio attento non nota però è che le coordinate del beneficiario sono state sostituite con altre coordinate di pagamento, spesso appartenenti ad un money mule, oppure a conti controllati dagli attaccanti e usati per far transitare le somme

Email security

Circa il 10% delle mail contiene un link, il link malevolo resta un efficace sistema di attacco, in crescita rispetto all'anno precedente. Rispetto all'invio del malware in allegato offre maggiori possibilità di evasione dei sistemi di email security, soprattutto quando la mail è inviata da un account legittimo (abusato) e il link punta ad un sito legittimo che è appena stato compromesso.

Tecniche di attacco utilizzate

È utile riportare le tecniche di attacco più comuni:

- **DOS (Distributed Denial of Service)**

Un attacco **DoS (Denial of Service)** è un attacco volto ad arrestare un computer, una rete o anche solo un particolare

servizio.

DNS Reflector attack è un attacco di tipo Distributed Denial of Service (DDoS) che abusa di server DNS open resolver e ricorsivi (recursive) inviando a questi ultimi pacchetti contenenti informazioni falsificate sull'IP di provenienza (IP spoofing).

- **I servizi VOIP (Voice Over Internet Protocol)**

I VOIP rappresentano una modalità di trasmissione di voce e traffico multimediale su reti IP dove **le comunicazioni vocali vengono convertite, pacchettizzate e trasmesse sotto forma di traffico dati**.

Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere dato che può sfruttare le sinergie con la rete dati. D'altra parte questo meccanismo è caratterizzato da possibili **vulnerabilità** (tipiche di una classica rete IP) e può ampliare la superficie d'attacco alla quale le Aziende sono esposte.

Le particolarità e vulnerabilità dello specifico protocollo possono infatti rappresentare un ulteriore modo per condurre attacchi mirati e frodi contro aziende e organizzazioni. Le problematiche sono varie: si può trattare di scenari evoluti di **Social Engineering** e intercettazione fino a possibili interruzioni di servizio **(DoS e DDoS)** e **Service Abuse** (dove l'infrastruttura della vittima viene utilizzata per generare traffico verso numerazioni a tariffazione speciale)."

Una blacklist è una lista dove vengono inseriti e catalogati indirizzi IP classificati come fonte di e-mail di SPAM.

Ci sono diversi motivi per cui si può essere inseriti nelle liste nere, di seguito cercheremo di analizzare i principali:

- Invio di e-mail massive dal proprio indirizzo.
    - Nel testo o nell'oggetto delle e-mail inviate sono

presenti caratteri e simboli in genere utilizzati nelle mail di SPAM

Il pc è infetto da virus che invia autonomamente e ciclicamente email infette.

- **Il fenomeno del Carding**

Con il termine Carding si identifica principalmente lo scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.

- **Attacchi tramite malware**

Le modalità di attacco da parte dei malware bancari rimane quella di tipo **Man-in-the-browser**, mediante **injection** di codice malevolo all'interno delle pagine web dei portali di **home banking**. La **web injection** può essere effettuata sulla pagina di login, allo scopo di rubare le credenziali di accesso al portale.

Quando l'utente visita l'home banking della propria banca il malware si attiva e resta in attesa che l'utente si posizioni nella pagina di login o di esecuzione dei bonifici. Appena il malware riesce ad entrare in possesso di una sessione valida tra il cliente e il portale della banca allora inizia la procedura per eseguire una frode mediante due possibili tecniche. In un primo caso il bonifico viene fatto partire in maniera automatizzata e in modo trasparente all'utente non appena quest'ultimo esegue il login sul portale della banca; di solito il bonifico necessita di un codice OTP per poter essere inviato quindi il malware richiede, mediante una tecnica di socia engineering, un secondo codice OTP durante la procedura di autenticazione.

Nel secondo caso l'operazione di bonifico iniziata da un cliente della banca viene intercettata dal malware e il

destinatario viene modificato prima di inviare la richiesta al server della banca senza che l'utente se ne renda conto. Il cliente rimane ignaro di quanto accaduto poiché il malware altera la struttura grafica delle sezioni interne del portale della banca per nascondere il bonifico fraudolento, ad esempio nelle pagine di conferma e successivo resoconto delle disposizioni effettuate. In alcuni casi il malware blocca le connessioni al provider di posta elettronica sul computer della vittima e rimuove ogni riferimento a numeri o chat di assistenza sul sito web della banca; in questo modo il malware ha più tempo a disposizione prima che la vittima riesca a contattare la banca per segnalare anomalie e bloccare la transazione fraudolenta.

- **Phishing / Social Engineering**

Tra i **numerosi toolkit di phishing che consentono di realizzare velocemente delle pagine di raccolta delle credenziali** ci sono quelli che emulano un portale di webmail dell'organizzazione a cui viene inviata la mail malevola.

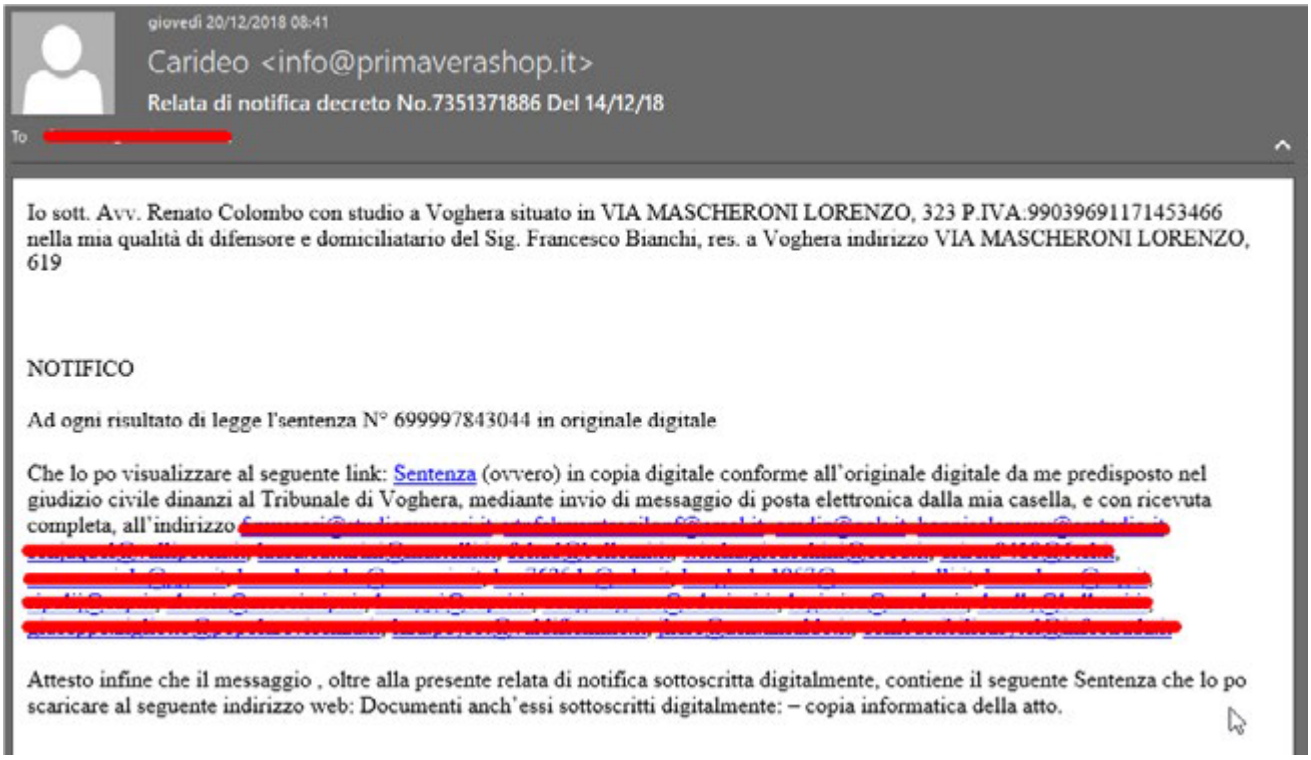
La pagina che richiede le credenziali cerca di apparire come un portale di webmail dell'organizzazione mostrando in modo dinamico nel titolo il nome del dominio dell'indirizzo email della vittima.

In "altri tipi di phishing viene preso come obiettivo una persona in particolare o un impiegato di una azienda specifica. Tale modalità fa sì che lo **spear phishing** diventi ancora più efficace e quindi pericoloso: **il cybercrime raccoglie informazioni relative alla vittima in modo tale che questa possa essere ingannata**. È infatti molto complesso distinguere un'e-mail di **spear phishing** ben ideata da una normale, per questo è più facile che le vittime cadano nella trappola".

You have new mail waiting

In molti casi analizzati, i malware sono stati **inseriti come allegati all'interno di conversazioni realmente avvenute tra la vittima e un interlocutore noto**. All'atto pratico, la vittima riceve una risposta ad un messaggio già scambiato, oppure un nuovo messaggio da una controparte nota, e il messaggio contiene un allegato malevolo. Questo modus operandi mira ad aumentare la fiducia della vittima nei confronti dell'allegato ricevuto, inducendolo ad aprire il file senza porsi troppe domande.

- Un esempio di mail riconducibile al *phisihing* è quello rappresentato nella figura sottostante. *"Si può notare che la mail prende di mira utenti italiani e, come numerosi casi simili riscontrati durante l'anno in diverse campagne, simula proprio l'invio di notifiche di atti giudiziari."*


giovedì 20/12/2018 08:41

Carideo <info@primaverashop.it>

Relata di notifica decreto No.7351371886 Del 14/12/18

To [redacted]

Io sott. Avv. Renato Colombo con studio a Voghera situato in VIA MASCHERONI LORENZO, 323 P.IVA.99039691171453466 nella mia qualità di difensore e domiciliatario del Sig. Francesco Bianchi, res. a Voghera indirizzo VIA MASCHERONI LORENZO, 619

NOTIFICO

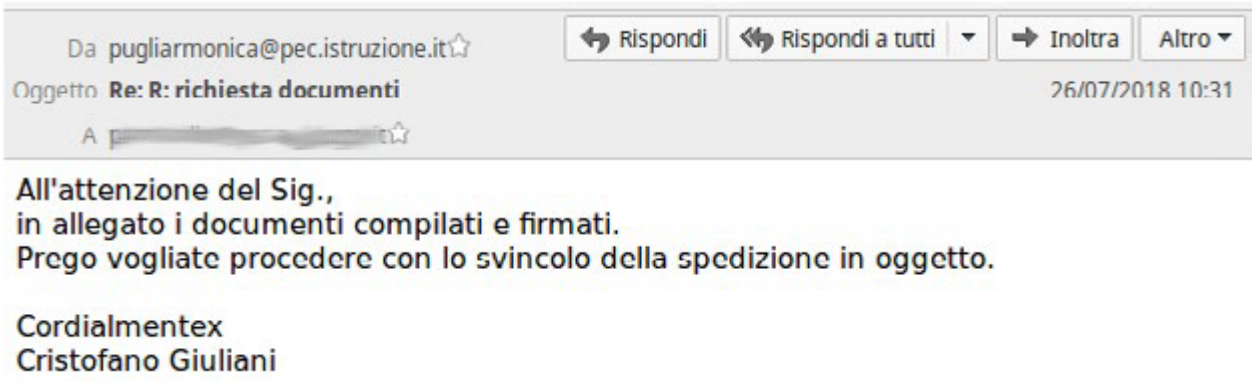
Ad ogni risultato di legge l'sentenza N° 699997843044 in originale digitale

Che lo po visualizzare al seguente link: Sentenza (ovvero) in copia digitale conforme all'originale digitale da me predisposto nel giudizio civile dinanzi al Tribunale di Voghera, mediante invio di messaggio di posta elettronica dalla mia casella, e con ricevuta completa, all'indirizzo [redacted]

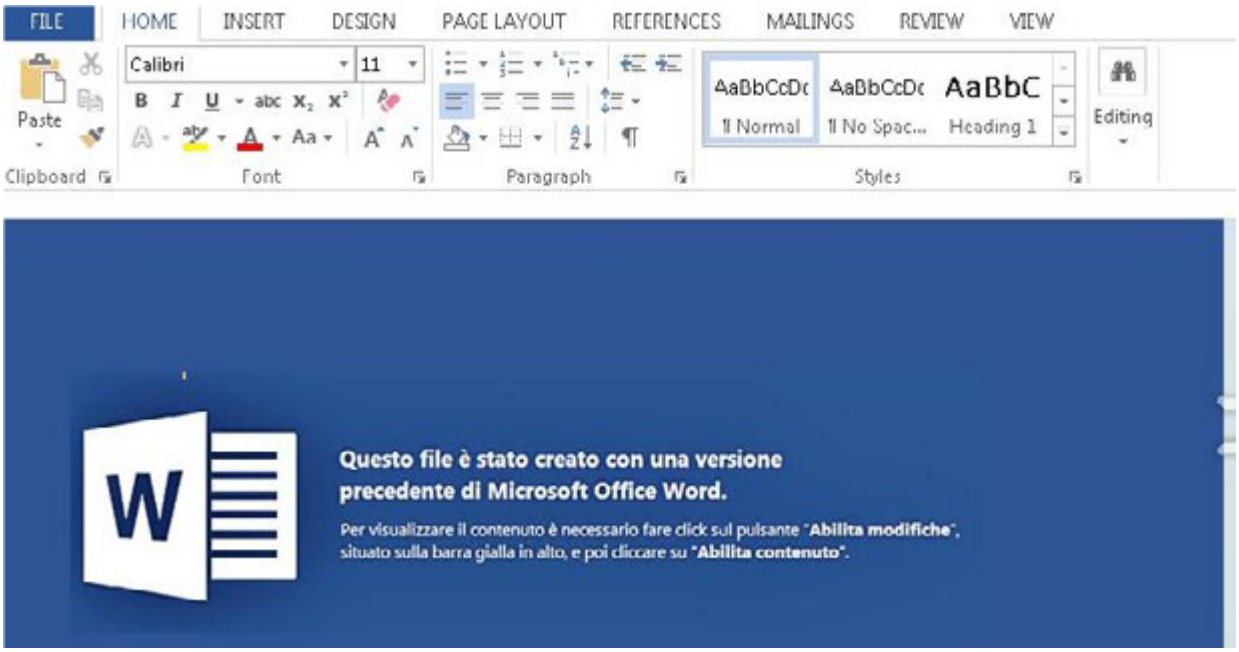
Attesto infine che il messaggio , oltre alla presente relata di notifica sottoscritta digitalmente, contiene il seguente Sentenza che lo po scaricare al seguente indirizzo web: Documenti anch'essi sottoscritti digitalmente: – copia informatica della atto.

- La mail di phishing può anche non contenere un link ma rimandare a un file allegato, [vedi figura sottostante]. Si tratta di un documento Word (in altri sample vengono

utilizzati anche file Excel) che, se aperto, presenta un messaggio di errore e invita l'utente ad attivare l'esecuzione delle macro per poter procedere alla lettura del documento.

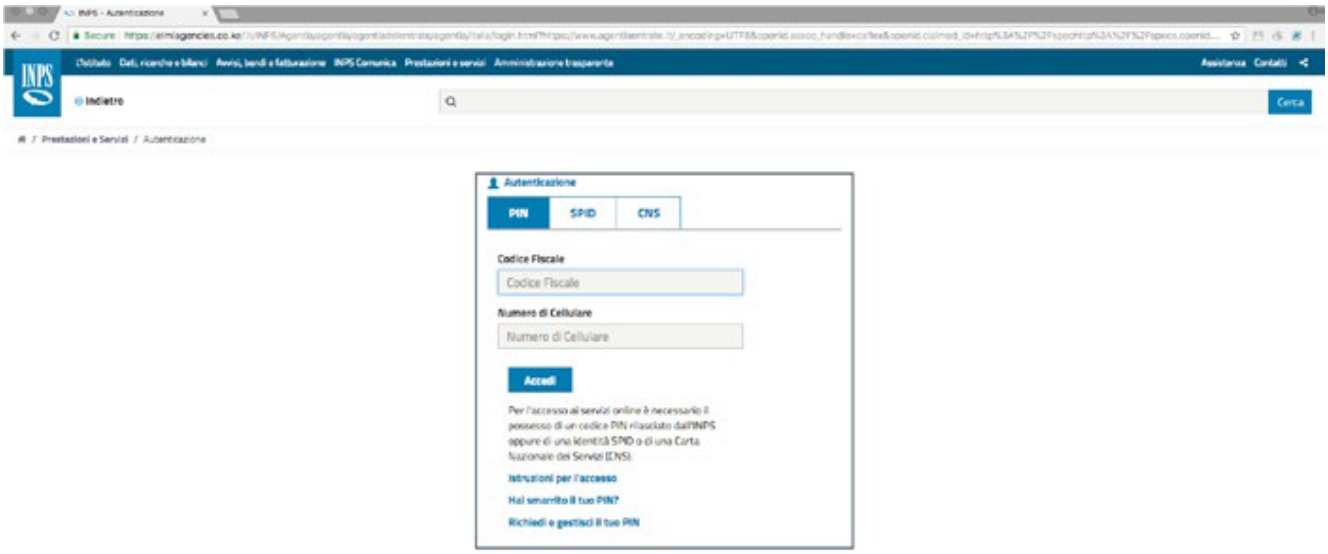


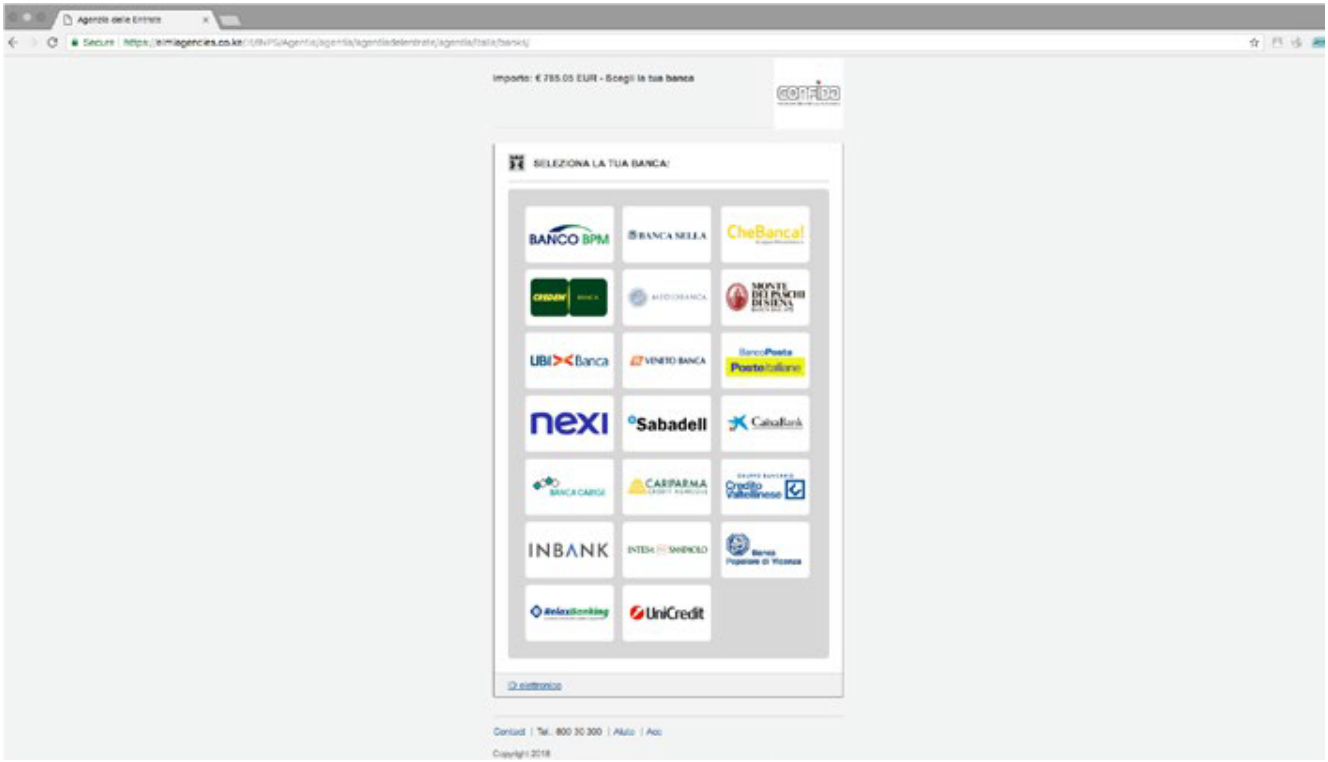
Il secondo passaggio è "*l'abilitazione dei contenuti da parte dell'utente comporta l'esecuzione delle macro configurate nel foglio Excel, che subdolamente avvia una connessione a un server remoto compromesso per effettuare il download di un eseguibile. Il file scaricato è il malware vero e proprio che viene eseguito, sempre dalla macro e attraverso l'uso di PowerShell, sull'host ormai infetto*."



- "***Numerosi casi relativi alle campagne osservate*** *durante l'anno appena trascorso e aventi come obiettivo solo l'Italia,* ***erano veicolati via PEC*** *e cioè un canale normalmente considerato affidabile*".

In tal senso una campagna di phishing particolarmente strutturata si è sviluppata nella prima metà dell'anno, provando a ingannare l'utente con un riferimento ad un finto rimborso INPS. La campagna era organizzata in modo da raccogliere prima i dati personali dell'utente vittima – codice fiscale e numero di telefono, [VEDI FIGURA sottostante] – e successivamente invitando l'utente a selezionare la propria banca – tramite cui ottenere il rimborso, [VEDI FIGURA sottostante] – prima di reindirizzarlo al finto sito web dei numerosi istituti bancari coinvolti per il furto vero e proprio delle credenziali di login.





- **PowerShell di Windows**

È il metodo di attacco con cui iniettare il malware all'interno di processi Windows in esecuzione in memoria e senza la necessità di scaricare file in locale, evadendo molti degli antivirus.

Applicazioni infette negli app store

Usare solo app scaricate da store ufficiali è certamente una pratica virtuosa, ma non risolve del tutto il problema.

BankBot è un malware Android, inserito all'interno di applicazioni apparentemente legittime, e con capacità di controllare lo schermo attraverso overlay. Il malware rimane silente all'interno dell'applicazione infetta fino a che l'utente non lancia sullo smartphone una delle app per accedere ai servizi di banking. A questo punto BankBot, prende il controllo dello schermo per catturare le credenziali utente.

Ma come fa il malware a finire su Play Store, raggirando i controlli di sicurezza? L'analisi

delle app infette con BankBot ha accertato che tutto comincia con una applicazione benigna, nei casi analizzati un'app contenente video comici o tutorial di cucito, caricata sul Play Store. Dopo che un certo numero di utilizzatori hanno scaricato e installato l'app, si invia un aggiornamento che istruisce l'app a scaricare altro codice, questa volta contenente il malware, attraverso una connessione HTTP diretta, dall'app a un server Internet predisposto."

Furto di credenziali di piattaforme

a supporto delle cripto-valute

Ormai tutti i principali malware, parallelamente agli obiettivi bancari, implementano tattiche per il furto di cripto-valuta.

Soluzioni per la Cyber Security

È indubbio che qualsiasi siano le soluzioni messe in campo dai fornitori di servizi finanziari, queste devono essere supportate da continua osservazione e ricerca dell'evoluzione delle tattiche di attacco. In un contesto mutevole come quello descritto, una soluzione non supportata da team di ricerca specializzati nell'analisi del malware, rischia di divenire presto obsoleta e inefficacie. Le soluzioni adottate devono altresì essere in grado di continue riconfigurazioni sulla base delle mutate forme di attacco. Ad esempio un SIEM deve adesso poter individuare utilizzi malevoli della PowerShell.

Indubbiamente, anche l'intelligenza artificiale e le capacità cognitive inserite all'interno delle singole soluzioni, saranno leve importanti nel campo della lotta al cybercrime nel settore finanziario.

L'uso dell'intelligenza artificiale nelle soluzioni di sicurezza offerte sul mercato si sta orientando su tre macro aree. Anzitutto nell'analisi predittiva con sistemi in grado di identificare autonomamente nuove frodi.

Su questo aspetto vede essere sviluppata l'area della *Intelligence Consolidation*, "che sfrutta le capacità di interpretazione del linguaggio naturale, analizzando e apprendendo dall'enorme quantità di informazioni, per lo più in forma non strutturata e prodotte continuamente nel campo della sicurezza.

Molto utile la ***"Security bulletins"*** cioè "report, grafici, conferenze, notizie di agenzia, tweet, advisories e altre

fonti, che altrimenti rischierebbero di finire ignorate in quanto non fruibili dalle soluzioni di sicurezza finora usate.”

Infine, l’Intelligenza Artificiale si pone come *trusted advisor* a supporto del lavoro degli analisti umani, per una più veloce risposta alle minacce e agli attacchi.

Non quindi una tecnologia che sostituisce il security analyst, ma piuttosto una tecnologia a supporto del security analyst, di cui incrementa sensibilmente la produttività.

Sviluppo di un sistema di *cyber threat intelligence*

L’attività di **CTI** è usualmente espletata da specifiche unità in seno a **CERT** (Computer Emergency Response Teams) o **CSIRT** (Computer Security Incident Response Teams). Uno scenario maturo prevede la gestione, suddivisa e coordinata, di attività tattiche di CTI e attività strategiche di CTI all’interno di un’unica struttura preposta.

Fondamentale il ruolo dei Security Operation Center (SOC) e di tutte le figure che in essi operano, come i Security Analyst, i Security Manager e i Network Specialist. A queste figure, con ruoli diversi, sono demandati i compiti controllo e investigazione sulle minacce, attacchi e vulnerabilità che colpiscono l’organizzazione, la sua infrastruttura, le applicazioni e i dati.

In questo contesto una piattaforma di **Threat Intelligence** è lo strumento fondamentaleper l’investigazione degli eventi di sicurezza, consentendo di verificare e confrontare allarmi, log, file binari, con una fonte autorevole e aggiornata, con lo scopo di confermare o escludere una potenziale minaccia.

Inoltre la piattaforma di **Threat Intelligence** permette la condivisione di informazioni tra membri dello stesso team,

oppure all’interno di team estesi accomunati dalla stessa necessità investigativa.

Per l’analisi tecnica di possibili *intrusions*, è utile l’impiego di **framework** strutturati come la **cyber kill chain (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions)** e il **diamond model (Adversary, Infrastructure, Victim, Capability)**.

Per l’identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere è efficace l’utilizzo della *course of action matrix* (composta da due azioni passive – **Discover** e**Detect** – e cinque attive – **Deny, Disrupt, Degrade, Deceive, Destroy**).

Per approfondire

https://www.key4biz.it/cybercrime-quali-sono-le-tecniche-dattacco-alla-luce-del-clusit-2019/255031/

Russian Hackers Use RATs to Target Financial Entities

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/7RPBRLHofJg/russian-hackers-use-rats-target-financial-entities

---

Mysterious Operative Haunted Kaspersky Critics

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/b44jQgFwMJs/mysterious-operative-haunted-kaspersky-critics