White Paper

Proteggersi efficacemente dai pericoli della rete

UN FALSO SENSO DI SICUREZZA 1

C'È TRUFFA PER TE 1

SITI IN OSTAGGIO E PUBBLICITÀ DAVVERO INGANNEVOLI 1

SIAMO TUTTI BERSAGLI 1

QUALI CONTROMISURE? 1

QUANDO IL RESTO NON È SUFFICIENTE 1

UN FALSO SENSO DI SICUREZZA

Difficile che trascorra qualche giorno senza che **i media non riportino notizia di qualche azienda**, ente pubblico o organizzazione a **cui dei cybercriminali abbiano razziato informazioni, sottratto denaro o bloccato i computer chiedendo un riscatto**.

Sono notizie che magari leggi con una punta di divertimento pensando che tanto no, ***a me non può succedere***.

In fondo mantieni i tuoi sistemi operativi sempre aggiornati, la tua azienda è dotata dei più moderni software di sicurezza e antivirus, la tua rete è protetta da sofisticati firewall e il tuo consulente IT vigila costantemente affinché tutto funzioni regolarmente.

Non puoi nemmeno accedere alla rete aziendale dal tuo smartphone personale né navigare su siti discutibili: *quindi* **devi proprio essere in una botte di ferro**.

Oppure no?

C'è una cosa che i media si dimenticano sempre di dire quando raccontano di campagne di attacchi e truffe informatiche andate a buon fine: che fino a quel momento anche le vittime avevano vissuto con la medesima sensazione di sicurezza, per le medesime buone ragioni.

Approfondisci le casistiche, e scoprirai che **le aziende colpite non mancavano certo né di firewall, né di software per la sicurezza, né di specialisti IT capaci**.

Ma allora perché i cybercriminali riescono a colpire con successo in modo così frequente?

Semplicemente perché hanno lasciato perdere gli attacchi puramente tecnici – computer contro computer, per intenderci – **concentrandosi invece sul vero anello debole della catena: l'essere umano**. Siamo noi e i nostri utenti, col nostro comportamento talvolta inconsapevole, spesso distratto, a permettere che gli attacchi informatici abbiano successo.

C'È TRUFFA PER TE

Uno dei principali canali di attacco di questo genere è **la posta elettronica**.

Sono sicuro che anche tu avrai ricevuto tantissime volte messaggi email scritti a nome di qualche istituto bancario, servizio di pagamento, sito e-commerce, corriere, utility, operatore Internet o altro brand conosciuto che invita, magari in un italiano stentato e zeppo di errori ortografici, a confermare le tue credenziali utente attraverso un link appositamente fornito, a scaricare una presunta fattura o a leggere attentamente le importanti informazioni contenute in un documento allegato.

Può sembrare incredibile, ma l'invio automatico di milioni di messaggi di questo genere attraverso vere e proprie campagne di spam è **diventato uno degli strumenti di maggior successo tra quelli usati dai malintenzionati digitali**.

Si tratta della tecnica nota come *phishing* – storpiatura dell'inglese *fishing*, pescare – che si basa sull'idea di **spacciarsi per un mittente noto** così da far abbassare il normale livello di cautela che tutti esercitiamo quando riceviamo messaggi non richiesti da perfetti sconosciuti, spingendo quindi l'inconsapevole utente a compiere un'azione capace di mettere in moto il meccanismo della truffa senza che ciò risulti evidente.

Una casistica di phishing assai comune è quella di **chiedere all'utente**, con la scusa di un account bloccato, **di verificare i propri dati personali** su un sito controllato dal truffatore.

Il messaggio email contiene un link che rimanda a **una pagina web dall'aspetto simile a quello del sito ufficiale** del preteso mittente, dove l'utente deve compilare un modulo con le informazioni richieste: username, password, data di nascita, codice fiscale e tutto quello che il cybercriminale intende carpire alla sua vittima.

L'utente poco accorto rivela in questo modo le credenziali che potranno essere utilizzate per accedere ai sistemi dell'organizzazione di cui si sono prese le sembianze, nonché altre informazioni riservate che potranno essere rivendute con profitto nel cosiddetto dark web.

Le mail usate per questi attacchi hanno un aspetto simile o identico a quello dei messaggi ufficiali inviati normalmente dall'organizzazione legittima, e nei casi più sofisticati i link eventualmente presenti rimandano a domini dal nome pressoché uguale, magari approfittando di similitudini tipografiche tra lettere differenti: è sufficiente sostituire una L minuscola con una I maiuscola o scegliere un dominio geografico simile (come *.lt*, Lituania, al posto di *.it*). **Il testo, sempre più spesso scritto correttamente in buon italiano**, segue esattamente lo stile grafico e formale delle comunicazioni del legittimo mittente, tanto che diviene sempre difficile capire quando ci si trova davanti a una mail fasulla.

Non ci è voluto molto perché le menti responsabili di questo genere di attacchi si rendessero conto che il meccanismo del phishing poteva essere messo meglio a frutto **personalizzandolo a livello individuale**. Ecco dunque che ai tradizionali invii automatizzati di massa verso enormi quantità di indirizzi email si è presto aggiunto un modo più subdolo per colpire: è il cosiddetto ***spear phishing***, termine che per l'appunto richiama la pesca all'arpione ("spear") dal momento che **il cybercriminale agisce dopo aver scelto con attenzione l'obiettivo**, averne studiato le caratteristiche e predisposto comunicazioni su misura.

Si tratta di un'applicazione customizzata delle tecniche tipiche del phishing, ed è proprio la sua personalizzazione a renderla ancora più letale aumentandone l'efficacia.

Attualmente è molto in voga una sua variante denominata **BEC (Business Email Compromise)**, conosciuta anche come "truffa del CEO".

Si tratta di un attacco altamente personalizzato che avviene impersonando per posta elettronica dirigenti, colleghi, fornitori, enti istituzionali o altri soggetti in rapporto d'affari con l'azienda che si intende colpire. Una truffa BEC ha solitamente lo scopo di sostituire l'IBAN di un creditore con quello di un cybercriminale e di dare illegittimamente corso a un mandato di pagamento a favore del malintenzionato, ma può essere sfruttato per furti di dati, spionaggio industriale e molto altro ancora.

SITI IN OSTAGGIO E PUBBLICITÀ DAVVERO INGANNEVOLI

Le brutte notizie non finiscono qui, perché **i rischi non si esauriscono con la posta elettronica**.

Oggi, infatti, l'ignaro **utente viene colpito mentre naviga tranquillamente sul web** pur tenendosi attentamente alla larga da siti di dubbia reputazione. Il motivo è che non è difficile incappare in **siti pienamente legittimi** – magari appartenenti a persone, aziende, associazioni, persino a enti pubblici – **che vengono violati** sfruttando vulnerabilità note dei sistemi con cui vengono realizzati: per esempio CMS come Wordpress, Joomla o Magento e relativi plugin non aggiornati, database insicuri o addirittura server mal configurati.

Una volta compromesso un sito, è davvero un gioco da ragazzi modificarne i contenuti per dirottare i visitatori verso siti ben più pericolosi o facendoli diventare un veicolo di malware.

Il problema è assai più diffuso di quanto non si creda perché tutta la procedura che parte dalla ricerca di un sito vulnerabile per arrivare all'iniezione di codice o contenuto malevolo viene svolta automaticamente da appositi software che "rastrellano" pazientemente l'intero World Wide Web dominio dopo dominio, sito dopo sito.

La rivista Security Magazine calcola che **sul web si verifichi mediamente un attacco ogni 39 secondi**; un'altra ricerca svolta da una società specializzata in sicurezza evidenzia come nel corso del 2019 sia risultato vulnerabile al punto di infezione oltre il 60% dei siti dei propri clienti[1].

Se tutto questo non fosse sufficiente, esiste anche un altro preoccupante fenomeno, quello del **malvertising** ovvero delle pubblicità online che contengono malware o rimandano a siti pericolosi. A volte pubblicità di questo genere riescono a superare i controlli anche delle società distributrici di advertising più quotate: gli operatori più seri sottopongono infatti ogni inserzione a verifiche di legittimità, ma talvolta gli hacker trovano il modo di aggirarle e allora sono guai.

Nel 2019, per esempio, un operatore truffaldino di Hong Kong è riuscito a stabilire partnership con le maggiori piattaforme pubblicitarie servendo oltre 100 milioni di inserzioni contenenti malware di vario genere attraverso siti web di alto profilo[2].

SIAMO TUTTI BERSAGLI

Molti si chiedono ancora a cosa serva tutto questo, se vi sia davvero un rischio nell'essere colpiti dal malware. Il ragionamento che sento ripetere spesso è: "Ma a chi vuoi che interessino i dati che ho sui miei computer?".

Sembra che le persone siano condizionate da certi pessimi film nei quali gli hacker sono invariabilmente interessati solo a ricchissime corporation globali o, in alternativa, al complesso industrial-militare di qualche nazione. La realtà è un'altra: tutti noi, in un modo o nell'altro, siamo potenziali bersagli. Nessuno può pensare di essere immune di fronte a un fenomeno che colpisce in maniera indiscriminata potendo profittare delle

1 https://sucuri.net/reports/2019-hacked-website-report/
2 https://threatpost.com/malvertising-campaign-100m-ads-supply-chain/146508/

proprie vittime nelle maniere più diverse:

- **Cryptomining**. La produzione di criptovalute come Bitcoin avviene in genere come una sorta di premio a fronte del completamento di un'enorme quantità di calcoli complessi. L'impegno richiesto è tale che un singolo PC potrebbe trascorrere anni a macinare calcoli senza ottenere alcun guadagno: ecco allora che sono stati inventati programmi di cryptomining che assemblano la potenza di grandi quantità di computer per riuscire a generare criptovalute in tempi brevi. La conseguenza per l'ignaro proprietario del PC colpito da un cryptominer è l'estrema lentezza del sistema, le cui risorse vengono principalmente assorbite dallo sgradito ospite.

- **DDoS**. Il Distributed Denial of Service è un attacco rivolto contro un sistema che viene contemporaneamente contattato con richieste di accesso o di traffico da migliaia di computer e dispositivi connessi al solo scopo di saturare la banda di comunicazione disponibile così da rendere inutilizzabile il sistema bersagliato. I cybercriminali hanno quindi bisogno di infettare grandi quantità di PC da mettere sotto il loro controllo (trasformandoli nei cosiddetti "zombie") per sfruttarli in azioni DDoS coordinate.

- **Keylogger**. Immagina di lavorare al computer avendo qualcuno che ti osserva costantemente da dietro le spalle. Un keylogger infatti è un piccolo programma appartenente alla categoria dello spyware (v. oltre) che si nasconde in profondità all'interno di un PC registrando tutti i tasti che vengono digitati dall'utente. I dati così raccolti vengono periodicamente inviati all'autore del keylogger che potrà così conoscere tutto quello che è passato per la tastiera dei sistemi colpiti: testi confidenziali, email inviate, ricerche Internet, credenziali.

- **Spyware**. Una particolare tipologia di malware che ha lo scopo di raccogliere quante più informazioni possibili sull'utilizzatore del computer o del dispositivo sul quale risiede. A differenza di altri malware, lo spyware è scritto per restare ben nascosto più a lungo possibile raccogliendo dati sensibili attraverso varie modalità come la lettura dei file memorizzati sulla macchina o le comunicazioni in entrata e in uscita a scopo di esfiltrazione o di profilazione dell'utente. Gli esemplari di spyware più sofisticati possono estendere il loro raggio d'azione anche alla rete alla quale è collegato il dispositivo infetto.

- **Spam**. Se credi che la popolazione mondiale si divida semplicemente tra chi riceve mail indesiderate e chi invece le spedisce, sei in errore. Esiste infatti una porzione di umanità che rientra in entrambe le casistiche, pur se inconsapevolmente: sono tutti coloro i cui computer sono stati compromessi da malintenzionati che li utilizzano per l'invio di spam. I PC colpiti in questo modo rallentano le prestazioni, comportano responsabilità legali e rischiano di essere buttati fuori dalle reti a cui si collegano. Oltre, naturalmente, al fatto che non si può mai sapere quale altro software illecito potrà essere successivamente installato da chi li controlla.

- **Ransomware**. Forse la più temuta tipologia di malware oggi esistente. Il ransomware crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete, backup compresi) che diventano così inaccessibili a meno di non pagare un riscatto (ransom) per ottenere la chiave di decifrazione necessaria. Tuttavia non sono rari i casi in cui anche la disponibilità di questa chiave non consente il ripristino corretto dei sistemi, con conseguenze di gravità direttamente proporzionale all'importanza dei file perduti.

Riepilogando quanto abbiamo visto finora **potremmo raffigurarci una sorta di piramide rovesciata**: in cima tutte le numerose e sempre crescenti varietà di malware, le quali poggiano sulle tecniche di diffusione analizzate in precedenza (la posta elettronica, la navigazione su siti infetti, il malvertising). Ancora più in basso c'è un unico elemento che rappresenta il vertice di questa piramide rovesciata, il vero punto di origine di tutta la catena d'attacco: **i link su cui gli utenti cliccano per scatenare l'infezione digitale**.

D'altra parte, **cosa sarebbe Internet senza i link**?

È proprio la natura della rete quella di permettere agli utenti di saltare da un contenuto all'altro, da un sito all'altro, da un sistema all'altro, da un servizio all'altro semplicemente con un clic. I malintenzionati lo sanno bene e quindi **puntano moltissimo sul fatto che una persona, per quanto possa essere attenta, prima o poi cadrà inavvertitamente nella trappola di qualche link maligno**. L'elemento umano è, in poche parole, l'anello debole da sfruttare per un attacco di successo: è sufficiente un clic, uno solo, sul link sbagliato (o giusto, dal punto di vista dell'attaccante) per scoperchiare un pentolone di problemi di non poco conto.

QUALI CONTROMISURE?

Ma allora non puoi far altro che aspettare che arrivi anche il tuo turno per essere colpito?

Fortunatamente no, prendendo le dovute precauzioni e **sfruttando in modo intelligente gli strumenti che la tecnologia mette a disposizione**.

Sgomberiamo subito il campo dai falsi miti e dalle errate credenze: **non esiste un'unica soluzione** che ci metta al riparo da tutti i pericoli del mondo digitale. Poteva esserci magari una trentina d'anni fa, nell'era pre-Internet, quando l'unico rischio che si poteva correre era quello di farsi infettare dai virus veicolati tramite qualche floppy disk e allora era sufficiente un buon programma specializzato per evitare spiacevoli conseguenze.

Oggi invece lo scenario è talmente variegato e dinamico che bisogna adottare una **strategia decisamente più organica e completa. In altre parole: contrapporre alla piramide rovesciata dei malintenzionati una ben più solida piramide tradizionale composta da strati di protezione ad hoc**.

E allora vediamo come è costruita una piramide del genere partendo dalle fondamenta. È qui che si trova il **firewall**, il guardiano che osserva il traffico di rete in entrata e in uscita assicurandosi che certe porte restino sempre ben chiuse, suonando l'allarme quando gli schemi di traffico si distaccano dalla normalità e, nei modelli più sofisticati, analizzando persino i dati circolanti per bloccare mittenti e/o contenuti sospetti.

Il firewall fa un gran lavoro ed è un elemento insostituibile in qualsiasi strategia di protezione informatica, ma anch'esso ha i suoi limiti: a volte qualcosa può passare attraverso le sue maglie atterrando, per così dire, sui sistemi oggetto dell'attacco. Qui è importante che i computer non presentino vulnerabilità note, né a livello di sistema operativo né a livello di applicazioni. Come saprai, è pressoché impossibile che software complesso come quello che usiamo oggi in tutte le nostre attività non contenga qualche errore di programmazione; alcuni di questi bug possono essere abilmente sfruttati dagli hacker per assumere il controllo del computer e da qui, attraverso procedure di escalation, anche dell'intera rete locale a cui la macchina è collegata. Per questo un'adeguata politica di **patching** che mantenga aggiornati i sistemi aiuta a ridurre enormemente la possibilità di approfittare di vulnerabilità di questo genere.

Saliamo di un gradino verso l'alto e troviamo uno strumento ormai tradizionale come l'**antivirus**.

Ovviamente è un parente lontano degli antivirus dei primi anni Novanta, cresciuto parallelamente all'evoluzione delle tecniche di attacco e oggi capace di andare oltre il semplice confronto delle cosiddette segnature (le "impronte digitali" dei singoli codici virali) per sfruttare motori euristici, tecniche di intelligenza artificiale e reti globali di sensori attivi H24.

La presenza di un antivirus all'interno dei nostri sistemi permette di intercettare gli ospiti indesiderati che riescono ad aggirare le linee di difesa precedenti: un esempio è il malware che sfrutta le vulnerabilità zero-day, ovvero vulnerabilità del tutto ignote che i programmatori responsabili non hanno ancora avuto modo di correggere. Casi del genere non sono troppo frequenti, fortunatamente, ma nemmeno così rari come tutti preferiremmo.

Fin qui le protezioni nei confronti della tecnologia, ma la piramide sale ancora con accorgimenti che hanno lo scopo di tutelare l'utente evitando che le sue azioni possano inavvertitamente provocare conseguenze nefaste.

Ci troviamo nello strato occupato dalle soluzioni **antispam** e **antiphishing**, che tengono d'occhio la posta elettronica per neutralizzare i tentativi di approfittare della disattenzione, della credulità e della buona fede delle persone. Se i livelli precedenti della nostra piramide avevano lo scopo di rafforzare la componente tecnologica, a questo piano si iniziano invece a prendere le difese dell'elemento umano, da sempre l'obiettivo preferito di abili truffatori e imbonitori.

QUANDO IL RESTO NON È SUFFICIENTE

Nel gioco degli specchi delle nostre piramidi di attacco e di difesa non sorprende che il **vertice dell'apparato protettivo debba essere dedicato ai link**.

L'abbiamo visto prima: il malware fa leva su una serie di canali di diffusione, i quali convergono sull'unico scopo di spingere le persone a cliccare su qualche link.

Rovesciando il modello, la tutela degli utenti si completa mettendoli al sicuro attraverso speciali **filtri di navigazione** che interpongono una barriera studiata in modo da disarmare i link pericolosi ovunque essi siano annidati: nei messaggi di posta elettronica, nelle pagine di qualche sito, persino all'interno di app e programmi vari.

Un filtro di navigazione, detto anche filtro DNS, si basa su un funzionamento molto semplice sfruttando il normale servizio che permette al nostro traffico in uscita di trovare il giusto indirizzo di rete del sito o della risorsa che intendiamo visitare. **Semplificando, potremmo definire questo servizio come una sorta di rubrica telefonica di Internet che associa un numero (l'indirizzo di rete) a un nome (il dominio). Il filtro di navigazione non fa altro che depurare la rubrica da tutti i numeri che rimandano a destinazioni rischiose** grazie a continui aggiornamenti.

In questo modo non corri il rischio di cadere in trappola nemmeno se clicchi inavvertitamente su un link pericoloso, come per esempio quello che può essere contenuto in un messaggio di phishing. Il filtro di navigazione è uno **strumento efficace per disinnescare alla radice l'elemento su cui si poggia l'intera piramide rovesciata** dei malintenzionati digitali, facendola crollare al suolo per la nostra serenità.

Da non sottovalutare un altro aspetto positivo dei filtri di navigazione che, risiedendo nel cloud, non richiedono l'installazione e la configurazione di software particolarmente complessi ma basta l'installazione un piccolo agente sui dispositivi da proteggere. Il vantaggio di un approccio di questo genere non va assolutamente sottovalutato, poiché di **fatto ci permette di applicare uno scudo di difesa contro i link pericolosi non solo alle risorse aziendali ma anche a laptop, smartphone e tablet personali, sia quando ci troviamo in ufficio che quando siamo a casa o in giro**, fuori dalla tutela del nostro firewall e magari stiamo lavorando con un dispositivo non aggiornato e privo di soluzioni antivirus.

Un filtro di navigazione completa la strategia di difesa multistrato che continua a essere necessaria e che possibilmente continuerà ad arricchirsi con nuove soluzioni in risposta alle future evoluzioni delle tecniche di attacco.

Non possiamo sapere oggi quali saranno i trucchi a cui ricorreranno ladri e truffatori informatici in futuro, ma possiamo costruire e ampliare la nostra piramide protettiva in modo da restare sempre al passo. **I filtri di navigazione resteranno comunque una componente essenziale della nostra sicurezza** grazie alla loro facilità d'uso, all'ampiezza del loro raggio d'azione e alla loro capacità di affiancarci seguendo le azioni quotidiane di noi utenti, anello ora un po' meno debole della catena.

Glossario

BEC Business Email Compromise – Una sofisticata truffa mirata che nella sua versione più diffusa assume l'aspetto di comunicazioni provenienti da un dirigente aziendale per convincere un altro dipendente a dare corso a pagamenti verso conti bancari riconducibili agli autori dell'illecito. Per dare credibilità alle richieste vengono spesso falsificati documenti ufficiali e creati domini Internet dal nome molto simile a quello delle aziende e degli enti coinvolti.

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

CMS Content Management System – Un'applicazione per webserver che permette di realizzare e pubblicare facilmente siti dinamici di ogni genere, dai blog personali ai siti aziendali, dai magazine online fino addirittura agli ecommerce. Esistono numerosi CMS per ogni piattaforma: alcuni esempi sono Drupal, Joomla, Magento, Microsoft Sharepoint, Prestashop e Wordpress. Ogni CMS possiede un proprio ecosistema di moduli e plugin che permettono di personalizzarne l'aspetto e arricchirne le funzionalità. Questi componenti supplementari tendono a essere più vulnerabili dei rispettivi CMS, e per questo sono oggetto di speciali attenzioni da parte degli hacker.

DNS Domain Name System – La tecnologia che permette di assegnare un nome di dominio a un indirizzo di rete numerico rendendolo facilmente memorizzabile. Il DNS è una specie di rubrica universale sempre aggiornata che tiene traccia dei nomi mnemonici di dominio insieme con la loro associazione ai relativi indirizzi IP.

Firewall – Un componente di rete che controlla il traffico da e verso un singolo sistema o una rete di computer. Il firewall osserva una serie di regole, configurabili dall'amministratore, per filtrare i pacchetti di rete in transito a seconda di tipologia, destinazione o contenuto. Un firewall può essere un dispositivo hardware, un componente esclusivamente software o un ibrido integrato sotto forma di appliance.

Malvertising – Il punto d'incontro tra malware e pubblicità (advertising). In genere, il malvertising è composto da inserzioni online che nascondono al proprio interno codice dannoso o che rimandano a siti pericolosi. Lo scopo degli autori di malvertising è quello di riuscire a superare i controlli dei publisher e delle reti pubblicitarie per far diffondere le loro inserzioni su siti affidabili, spesso anche di fama e visitati da milioni di utenti di tutto il mondo.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza dello spear phishing e delle truffe BEC, che si basano su una accurata personalizzazione, il phishing si avvale di invii di messaggi in massa.

Spear phishing – Una variante del phishing estremamente personalizzata sul destinatario del tentativo di truffa. A differenza del normale phishing, i messaggi sono realizzati su misura dopo aver studiato il profilo della potenziale vittima attraverso le informazioni normalmente reperibili sul Web. Un accurato lavoro di preparazione permette di aumentare notevolmente l'efficacia dei messaggi prendendo alla sprovvista anche coloro che normalmente prestano poco credito alle comunicazioni indesiderate provenienti per posta elettronica..