Email security e minacce "Zero Day" - La posta elettronica come principale vettore di recapito per ransomware, malware o phishing

Date : 25 gennaio 2018

In base all'esperienza maturata nella sua azienda in ambito di e-mail security, quali ritiene che siano attualmente le cyber minacce più diffuse?

Dobbiamo sicuramente riferirci alle minacce 'Zero Day': sono minacce fino a poco tempo fa ignote, che trovano nelle e-mail il principale vettore di recapito per *ransomware*, *malware* o *phishing*. Essendo il canale prevalente della comunicazione aziendale, le mail lo sono anche per il malware e altre minacce: oggi questo tipo di attacchi è diventato la norma e quindi lavorare sulla sicurezza significa avere la capacità di bloccare minacce ignote.

Io mi occupo di Ricerca e Sviluppo in Libra Esva, un'azienda italiana che lavora appunto con l'e-mail security; ogni mese i nostri sistemi processano - solo per quanto riguarda l'Italia - oltre un miliardo di e-mail e oltre un milione di link (parliamo naturalmente dei link che sono presenti nelle mail). Sappiamo che è importante conoscere a fondo la tipologia di traffico per poterla filtrare correttamente; i nostri clienti appartengono a un target molto eterogeneo (andiamo dal traffico istituzionale a quello universitario, dal SB/SP al comparto industriale, fino alle piccole e grandi aziende) e di conseguenza abbiamo una visibilità molto ampia su quelle che sono attualmente le principali minacce in circolazione.

Parlando di *ransomware*, com'è cambiato negli ultimi anni il panorama relativo a queste minacce?

Oltre a un business da centinaia di milioni di euro l'anno (probabilmente ha già superato il miliardo) si è ormai creato un indotto, una sorta di "terziario" del malware, dove vengono offerti servizi che mettono in grado chiunque di realizzare la propria campagna di *phishing*, di organizzare e distribuire il proprio *ransomware*, di gestire i pagamenti avvalendosi di questi servizi. Esistono anche meccanismi di affiliazione per cui io posso acquistare un kit di sviluppo, realizzare il *malware*, distribuirlo attraverso una *botnet* in affitto e avere anche chi gestisce pagamenti e *customer care*, spiegando all'utente come dotarsi di bitcoin per effettuare i pagamenti. C'è tutto un lead di servizi che abilita sempre più persone, dotate di competenze

tecniche sempre meno profonde, a operare in questo settore estremamente lucrativo.

Nel 2016 abbiamo potuto osservare oltre 109 famiglie di *ransomware*; ogni famiglia dà origine a una grande quantità di varianti, proprio grazie a questi kit di sviluppo per cui ciascuno personalizza il proprio malware e lo distribuisce. Di conseguenza, ecco che nascono decine - o centinaia, dipende dai periodi - di nuove minacce ogni giorno e questo manda in crisi gli approcci classici basati sui *pattern* o sul *fingerprinting*, perché bloccare le minacce note non è più sufficiente: certo bisogna farlo (e ormai lo fanno più o meno tutti) ma oggi la vera sfida è essere in grado di bloccare le minacce di provenienza ignota.

Ipotizziamo un tipico attacco basato su una minaccia del giorno 0: il vettore è una mail che arriva da un mittente apparentemente legittimo, usato abusivamente grazie a credenziali rubate. Queste mail normalmente includono un link - che è quello che attiverà il *malware* - o un allegato con un contenuto malevolo al suo interno. I *Data base leak* sono ormai all'ordine del giorno e, grazie al fatto che la gran parte degli utenti utilizza le stesse credenziali per i diversi account, i *leak* di servizi come Yahoo o Linkedin danno accesso, spesso, anche alle credenziali della casella di posta dell'utente. Ormai le *botnet* non inviano più queste mail dal proprio indirizzo IP collegandosi all'SMTP server del destinatario, ma ricevono dal centro di comando e controllo una serie di credenziali che hanno queste origini; di conseguenza le mail arrivano da utenti legittimi (con cui magari intratteniamo una regolare corrispondenza) e diventa molto più difficile intercettarle.

Le credenziali non arrivano solo dai *data base leak* ma anche da attacchi 'a forza bruta', veicolati da macchine infette. In entrambi i casi abbiamo a che fare con un ignoto e i link normalmente puntano a un sito legittimo che è stato compromesso pochi minuti prima; la campagna parte al momento della compromissione per cui, nel momento in cui la mail arriva, nessuna fonte pubblica può ancora aver indicato quel sito come rischioso.

Cito un esempio, una mail che arrivava da un mittente legittimo e che puntava a un sito (registrato appositamente per questa campagna di *phishing*) identico a quello di MediaWorld, con tanto di certificato SSL ospitato su register e carrello funzionante, con l'obiettivo di raccogliere i dati delle carte di credito degli utenti. Ricordo poi una campagna - che si ripete periodicamente - che puntava a una copia della webmail dell'Università di Milano: un *phishing*, questo, estremamente mirato. Finché continueremo ad utilizzare gli strumenti tradizionali, come le Honeypot o le spam trap, non riusciremo a rilevare queste campagne così specifiche. Un altro esempio classico, sarà capitato a tutti; un *phishing* (sempre italiano) che puntava ad un finto sito di ING, una copia pressoché perfetta con i certificati in regola, che invitava a loggarsi per risolvere un problema di sicurezza. L'utente inseriva le proprie credenziali e c'era qualcuno che entrava nel conto corrente in tempo reale; nell'attesa venivano chiesti dati aggiuntivi (ad esempio quelli della carta di credito) e alla fine veniva chiesto il codice di conferma ricevuto via sms, quello originale inviato da ING, che serviva ad autorizzare il bonifico fatto per svuotarci il conto corrente.

Questo è un tipo di *phishing* che produce un guadagno monetario diretto, a differenza di quelli citati in precedenza che mirano a raccogliere dati di carte di credito per poi commercializzarli. Come dicevo le varianti sono innumerevoli, per questo abbiamo bisogno di strategie nuove: la

security deve evolversi per fare fronte a minacce sempre più capillari.

Quali sono le principali vulnerabilità che espongono le aziende a questo tipo di attacchi - e come è possibile contrastarli?

Per diffondere *malware* vengono essenzialmente in gioco due fattori: quello tecnico e quello umano. Quello umano continua ad essere definito l'anello debole della catena, anche perché esistono carenze di ordine tecnico che lo rendono tale. Ormai il *malware* che si auto-diffonde, che si trasmette autonomamente da macchina a macchina, è molto raro: è sempre necessaria la collaborazione umana ma si tratta di una collaborazione limitata, nel senso che è sufficiente cliccare su un link, o aprire un allegato, per essere infettati. La vulnerabilità di base è dovuta alla grande complessità dei sistemi che utilizziamo. Operazioni banali che tutti ripetiamo decine o centinaia di volte al giorno, se fatte sul file o sul link sbagliato, possono attivare l'infezione.

Il *malware* per sfruttare il fattore umano ha bisogno di alcune componenti: è necessario spacciarsi per una fonte autorevole e c'è bisogno di catturare l'attenzione (l'utente deve leggere la mail, quindi questi messaggi contengono sempre una *call to action* in grado di instillare un senso di urgenza). Questi fattori devono essere tradotti in qualche modo; i nostri sistemi cercano di identificarli e intercettarli per classificare le mail perché, in presenza di queste componenti, possiamo essere tutti vulnerabili.

Per dimostrarlo l'anno scorso abbiamo fatto un esperimento (è una cosa che funziona molto perché, quando verifichiamo che noi stessi possiamo "abboccare", la nostra sensibilità e la nostra attenzione aumentano e questo ci incentiva a lavorare sulla prevenzione). In occasione di un evento dedicato alla sicurezza informatica, abbiamo deciso di realizzare una campagna di *phishing* e valutarne l'efficacia. Prima dell'evento abbiamo inviato a tutti i partecipanti una mail - una copia sostanzialmente esatta di una richiesta di contatto di Linkedin - che puntava a una landing *page* realizzata acquistando il dominio più simile a quello originale. Abbiamo utilizzato uno strumento chiamato *Gophish*, uno dei tanti che esistono per realizzare queste operazioni, che aiuta a costruire il *template* della mail e la landing page, ha un server che *serve la landing page* e una parte analitica che misura in tempo reale le aperture e i click. In questa campagna ci eravamo dati come obiettivo far cliccare i destinatari sul link malevolo; avevamo anche documentato tutte le vulnerabilità uscite la settimana precedente negli aggiornamenti mensili di Microsoft, che potevano essere sfruttati con un semplice click. Il 40% dei destinatari è caduta nella trappola: e parliamo di un target di un certo tipo - non certo utenti sprovveduti ma persone che si occupano quotidianamente di sicurezza. La ritengo una conferma di quanto anticipavo: il *phishing*, se fatto in un certo modo, può trarre in inganno anche chi si considera al sicuro.

Cosa si intende per *whaling*?

Il *whaling* è un tipo di *phishing* specializzato. Ultimamente siamo passati dal *phishing* di massa, che invia messaggi di qualità bassa a tutti cercando di 'pescare nel mucchio', a campagne sempre più mirate. Così sono nati lo *spear phishing* - che studia la vittima cui inviare il messaggio - e il *whaling*, che ne rappresenta un'ulteriore specializzazione: qui la vittima viene studiata attraverso i suoi profili social e le vengono inviati messaggi spacciandosi per un

dirigente dell'azienda. Di norma l'obiettivo è indurre l'amministrazione a fare un bonifico o un'altra transazione; anche qui si fa leva sul senso d'urgenza, sulla fonte autorevole e su una *call to action* credibile. Queste campagne di *whaling* si sono diffuse a livello sempre più capillare tra aziende di ogni dimensione; ma mentre se viene colpita una grande realtà la notizia finisce sui giornali, ogni giorno ci sono campagne di *whaling* contro aziende medie o piccole che vanno a buon fine ma restano sotto il radar.

Per questo noi di LibraEsva abbiamo sviluppato un engine specifico, perché qui abbiamo ancora meno informazioni per poter definire come malevola la mail che tipicamente inizia con un messaggio del tutto generico («Ciao, sei in ufficio? Ho bisogno di te») e serve per sondare se la mail arriva al destinatario, se questi non si accorge che l'interlocutore si spaccia per il suo capo; se arriva la risposta la campagna prosegue e nel giro di due o tre scambi si arriva alla richiesta di un bonifico urgente da fare subito (perché «il cliente è arrabbiato», perché c'è la transazione in corso e così via). L'engine che abbiamo sviluppato richiede una configurazione minima, non prevede conoscenze specifiche del protocollo e riesce a intercettare anche questo tipo di minaccia. Questo per spiegare come bisogna far sì che le difese evolvano rapidamente in relazione a questo cambio nelle modalità di attacco.

Quali ritiene i principali fattori di ostacolo alla piena implementazione di adeguate *security policies* aziendali? In che modo le proposte LibraEsva si differenzierebbero dalle altre soluzioni sul mercato?

Dopo il fattore umano, bisogna considerare il fattore tecnico; e qui ci troviamo, purtroppo, nella contesa tra marketing e sicurezza. Quello della security è un mercato in grande crescita e determinati messaggi di marketing sono più efficaci di altri: quelli più efficaci dal punto di vista del marketing sono, di solito, in contrasto con la sicurezza reale. Nella sicurezza (anche quella fisica) la soluzione ideale è sempre quella che comporta la minore complessità per raggiungere un determinato obiettivo. Il problema è che si ritiene che una maggiore complessità faccia vendere di più. Perciò vediamo messaggi focalizzati sulla complessità, soluzioni con Intelligenza artificiale, sand*boxing*, *machine learning*, che dal punto di vista del marketing funzionano; ma grossi problemi di sicurezza sono legati proprio alla complessità dei sistemi che utilizziamo. I nostri sistemi sono estremamente complessi e quindi hanno un'estesa superficie di attacco: i sistemi che mettiamo a loro protezione dovrebbero avere un'impostazione diversa.

Noi di LibraEsva non ci siamo voluti far trasportare troppo dal marketing. Prendiamo ad esempio il sand*boxing*: strumento eccezionale per fare *malware analysis*, ma quando lo usiamo come filtro *real time* per gli allegati delle mail comincia a presentare problemi dovuti all'estrema complessità del sistema - è più complesso dei sistemi che vuole difendere, quindi molto più vulnerabile e con una superficie di attacco enorme. Infatti abbiamo già visto come le tecniche di evasione dalla sand*box* siano pressoché illimitate; ogni giorno c'è una nuova tecnica di evasione, ogni giorno c'è una risposta e di fatto siamo nella stessa situazione di prima, nel senso che abbiamo spostato l'eterna contesa tra chi attacca e chi difende ma il paradigma resta lo stesso; non riusciamo ad arrivare a 'tagliare le gambe' alle possibilità di attacco.

Per questo il nostro approccio al sand*boxing* è stato rinunciare a messaggi accattivanti dal

punto di vista del marketing, rimanendo su soluzioni più pragmatiche ed efficaci. Tra l'altro la soluzione sand*boxing* ha degli svantaggi oggettivi - ritardi nella consegna delle mail, fuoriuscita di informazioni riservate all'esterno dell'organizzazione. Noi abbiamo progettato una sand*box* che gira sul gateway di posta, che lavora in parallelo al controllo antispam (quindi non introduce alcun ritardo) per identificare eventuali codici attivi all'interno dei documenti, classificarli e in base alla classificazione eseguire un'azione che può essere lasciarlo passare, disarmarlo o bloccarlo; se non sono definiti *safe*, il codice viene disarmato. Di conseguenza, il file Pdf con javascript che fa accessi a internet viene consegnato senza codice; il documento Office contenente macro che fanno operazioni anomale, come accedere al file system o alla rete, viene consegnato senza le macro. Diventano documenti fruibili, ma disarmati del loro potenziale dannoso.

Questo approccio ha dimostrato di funzionare, abbiamo visto diverse campagne che pur implementando tecniche di evasione della sand*box* non riuscivano a superare i nostri controlli.

E per quanto riguarda il controllo sulle URL?

Le URL sono un problema ben diverso: innanzitutto è importante guadagnare tempo, perché come dicevo il sito magari è stato infettato 10 minuti prima della mail e al momento della sua apertura questa compromissione non è ancora nota. Per questo abbiamo adottato un approccio più complesso, sempre seguendo il ragionamento per cui aggiungo complessità solo laddove ne ho bisogno per raggiungere il mio obiettivo. Quando la mail arriva sul gateway, io riscrivo la URL e posticipo l'analisi di quel link al momento in cui verrà cliccato, ovvero l'ultimo momento utile in cui mi posso proteggere. In seconda battuta, nel momento in cui l'utente clicca su quel link, passa sulla sand*box* che in quel momento va a visitare il sito, analizza i *redirect* e il codice, lo visita da più *location* per verificare se ci siano tecniche di evasione. Il *malware* sul web si deve nascondere ai motori di ricerca e dalle sandbox, quindi se una richiesta arriva da un data center fornisco un contenuto diverso da quello fornito se la richiesta arriva da un ADSL consumer. Deve avere tecniche di offuscamento del codice, tecniche di *encryption*. Sono tutte cose che il malware ha bisogno di fare se vuole sopravvivere, ma che rivelano la sua presenza: il solo fatto di mettere in atto una tecnica di evasione evidenzia la presenza del *malware*. Anche se quello specifico *malware* è ignoto, non so come funziona ma so che c'è, si nasconde dai data center e si manifesta solo sugli ADSL.

Sul web invece il *malware* si deve manifestare immediatamente, non può aspettare mezz'ora prima di agire perché nessuno resta su una pagina web così a lungo: questo significa che tutti i controlli - che sono centinaia - avvengono in media in un secondo e mezzo, così introducendo un ritardo minimo nella navigazione web.

Sul web il fatto che le tecniche di evasione rendano più evidente il malware mi permette di giocare in vantaggio, diversamente dalla sand*box* basata sul *virtual machine* che analizza i file: lì è il *malware* che gioca in vantaggio, perché la sand*box* ha a disposizione solo due minuti e in quei due minuti esistono tantissime tecniche per non farsi scoprire.

Per concludere, quale ritiene l'approccio vincente per tenere il passo di

minacce in continua crescita ed evoluzione?

Il concetto di fondo è sempre quello: adottiamo un approccio pragmatico, cerchiamo di interrompere quest'eterna contesa tra chi attacca e chi difende, immaginiamo soluzioni più definitive, perché magari perderemo qualcosa sul fronte del marketing nel breve periodo ma guadagneremo reputazione sul lungo termine. E ci terremo i clienti, che invece di continuare a saltare da un *vendor* all'altro (che magari gli promettono la soluzione magica per poi lasciarlo più vulnerabile di prima) ci resteranno fedeli.

Come ultimo esempio, da alcune settimane a questa parte circola un *malware* che sfrutta il DDE. Alcune varianti ancora oggi vengono fatte passare da quasi tutti gli antivirus, mentre grazie a questo approccio basato sul *white listing* noi di LibraEsva siamo stati i primi - a livello mondiale - a bloccarlo con successo.

A cura di: **Rodolfo Saccani,** *Security R&D Manager in Libra Esva*