MISSION SECURED.

Next Generation security per proteggere l'azienda da qualsiasi tipo di cyberminaccia.

#TRUECYBERSECURITY

LA VOSTRA AZIENDA È PROTETTA?

Pochi settori dipendono dalla fiducia dei clienti quanto il settore dei servizi finanziari. Tale fiducia ha le sue fondamenta sulla percezione della sicurezza. L'approccio Kaspersky Lab True Cybersecurity combina una sicurezza multilivello con threat intelligence assistita dal cloud e machine learning per proteggere l'azienda da qualsiasi tipo di minaccia si trovi ad affrontare.

MAGGIORI OPPORTUNITÀ, SFIDE PIÙ GRANDI

Le tecnologie online e mobili hanno trasformato i servizi finanziari, aprendo nuovi canali di opportunità e incentivando l'innovazione per prodotti e servizi.

Dalla riduzione dei costi, alla flessibilità del cliente, ai servizi a valore aggiunto fino alle opportunità multicanale, la tecnologia è diventata un fattore chiave della fidelizzazione del cliente in un momento in cui i fornitori di Next Generation si stanno impegnando enormemente per attirare nuovi clienti con prodotti e servizi innovativi.

Purtroppo, le stesse tecnologie che consentono la flessibilità del cliente facilitano anche truffatori e cybercriminali. L'integrazione di servizi fisici e virtuali, la disponibilità delle informazioni di identificazione personale attraverso più fonti e la debolezza di software ampiamente utilizzati si uniscono al semplice errore umano consentendo frodi precedentemente inimmaginabili.

In un mondo in cui i cybercriminali possono raccogliere 100 milioni di dollari utilizzando credenziali SWIFT rubate per effettuare trasferimenti di denaro fraudolenti[1], in cui gli ATM possono essere violati per eseguire il rollback dei saldi[2] e gli attacchi di malware finanziari su computer e dispositivi mobili sono costantemente in aumento, proteggere l'autenticità delle transazioni digitali e le persone dietro di loro non è mai stato più impegnativo.

La disponibilità 24 ore su 24 è funzionale tanto per i clienti quanto per gli aspiranti ladri. Ed è più probabile che, al giorno d'oggi, una rapina in banca avvenga tramite l'attacco alla sicurezza di un laptop e non attraverso l'irruzione di una banda armata all'interno dell'edificio bancario stesso. I cybercriminali sono anche molto bravi a fingersi clienti legittimi.

Per contrastare queste minacce, i fornitori di servizi finanziari devono diventare agili quanto i cybercriminali. Sono essenziali soluzioni di cybersecurity scalabili e adattabili che utilizzano la più recente threat intelligence. Ma con così tanti canali da proteggere, è importante che la cybersecurity non aumenti la complessità o crei problemi di gestione e distrazioni.

DENARO VELOCE, MAGGIORI PROBLEMI

I pagamenti in tempo reale possono essere comodi per i clienti, ma possono anche causare enormi problemi alle istituzioni finanziarie: circa il 50% delle richieste di pagamento rapido quotidiane degli Stati Uniti può essere fraudolento.[3]

[1] Threatpost "Gli hacker del Bangladesh hanno violato il sistema SWIFT per rubare, coprendo le proprie tracce" (Bangladesh Hackers Accessed SWIFT System to Steal, Cover Tracks).
[2] Securelist: Le rapine in banca in stile APT sono aumentate con attacchi Metel, GCMAN e Carbanak 2.0 (APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks)
[3] Gartner Blog "Le frodi colpiscono i pagamenti in tempo reale: le rapine SWIFT si ripetono?" (Fraud hits U.S. real time payments; SWIFT heists repeated?)

IL CLIENTE È SEMPRE REALE?

Di fronte a regolamentazione, responsabilità e rischi maggiori e a una crescita esponenziale delle minacce informatiche, l'impatto delle frodi online e di altri cybercrimini sulle banche si estende ben oltre il solo risarcimento del cliente.

Mentre le stime sui costi variano ampiamente, ciò che è chiaro è che la percentuale di utenti che subiscono attacchi da frodi online e malware finanziari è in aumento: nel 2017, il 24% delle banche afferma che è difficile verificare l'identità di chi accede a servizi di online banking; il 37% delle banche ritiene che i propri clienti usino connessioni a Internet non sicure.[4] Il 48% di tutti gli attacchi di phishing registrati da Kaspersky Lab ha specificamente preso di mira dati finanziari degli utenti.

Non si tratta solo di phishing. Delle 30 famiglie note di Trojan bancari, oltre il 90% degli attacchi sferrati nel periodo delle vacanze del 2016 ha usato gli stessi cinque malware[5]. Tuttavia, nuovi Trojan e modifiche funzionali a quelli esistenti emergono costantemente. I cybercriminali utilizzano queste tecniche per un motivo semplice: funzionano.

Le minacce informatiche finanziarie sono in continua evoluzione, dato che i criminali alterano le tattiche esistenti o ne sviluppano di nuove nel tentativo di stare al passo con le tecniche di mitigazione.

Dal furto delle credenziali alla manomissione delle transazioni, passando per spoofing, siti web fittizi e tentativi di phishing, gli attacchi informatici sui servizi finanziari digitali hanno dato vita a un dilemma che sia fornitori di servizi che clienti si pongono: come posso esser certo che tu sia chi sostieni di essere?

FINGERE PER RAGGIUNGERE L'OBIETTIVO

Da tempo le banche sanno di avere bisogno di una sistema di autenticazione efficace, soprattutto quando si tratta di richieste di pagamento.

Per assicurare che solo gli utenti autenticati e autorizzati potessero richiedere i pagamenti, sono stati utilizzati sistemi a doppia autorizzazione e con altri tipi di controlli. Ma cosa succede quando i criminali utilizzano le credenziali originali, rubate durante gli attacchi informatici?

1.126.701

il numero di volte che le soluzioni Kaspersky Lab hanno bloccato tentativi di lanciare malware per il furto di denaro tramite servizi di online banking nel 2017.[6]

Una volta ingannato il cliente, per i criminali è facile raccogliere informazioni sufficienti a convincere i sistemi bancari di essere veri e propri clienti. Non è un caso se sono in aumento fenomeni come malware web injection e Man-in-the-Browser, in cui i criminali modificano un sito finanziario legittimo con campi fraudolenti di inserimento dati, false schermate o falsi messaggi di errore di transazione, come Carberp e Neverquest.

I cybercriminali sono diventati talmente abili nello sviluppo di malware in grado di rubare le credenziali di accesso che spesso è difficile individuare un cliente falso prima che avvenga la frode. Zbot Trojan, ad esempio, intercetta le sequenze di tasti o acquisisce schermate delle informazioni sensibili dei clienti dai computer infetti. È talmente efficace che ha occupato il primo posto nella lista dei malware finanziari "più usati" per vari anni; nel secondo trimestre del 2016, il 15% degli attacchi malware finanziari ha riguardato questo Trojan[7].

[4] Kaspersky Lab: nuove tecnologie, nuove cyberminacce, analisi dello stato di sicurezza IT nel settore finanziario 2017 (New Technologies, New Cyberthreats, analyzing the state of IT Security in the financial sector 2017)
[5] https://securelist.com/analysis/publications/77045/holiday-2016-financial-cyberthreats-overview/
[6] Kaspersky Security Bulletin statistiche generali per il 2017
[7] Rapporto di Kaspersky Lab IT sull'evoluzione delle minacce per il secondo trimestre 2016

TECNICA CONTRARIA: FINGERSI IL PERSONALE

Non c'è da preoccuparsi solo dell'autenticità del cliente, i cybercriminali sono abili anche a fingersi parte del personale dei servizi finanziari. Le tecniche utilizzate sono sempre molto simili:

PANORAMICA DI UN ATTACCO

1 Il dipendente viene indotto ad aprire e-mail di phishing o a visitare un sito nocivo e il malware infetta il sistema.

2 Il malware ruba le credenziali, si diffonde ad altre macchine sulla rete e va in cerca di un sistema con privilegi di amministratore.

3 Viene lanciato un ulteriore malware in grado raccogliere silenziosamente altre informazioni, come schermate di sistemi di trasferimento di denaro e altre credenziali.

4 Ora i criminali conoscono il modo in cui lavora il personale e possono accedere ai vari sistemi, sono pronti...

I quattro passaggi descritti potrebbero sembrare semplici, ma rappresentano il percorso utilizzato nel più famoso cyberfurto: Carbanak. Scoperto (e ora bloccato) da Kaspersky Lab, Carbanak ha portato al furto di oltre 1 miliardo di dollari da parte di cybercriminali. Questi hanno compromesso i sistemi del personale e ne hanno preso il posto simulandone le attività e trasferendo denaro tramite banking online, sistemi di e-payment, controllando gli ATM, ingigantendo i saldi dei conti e manipolando i database al fine di modificare i dettagli di proprietà.

Dal cyberfurto Carbanak, abbiamo assistito a Carbanak 2.0, Metel e GCMAN. Tutti questi attacchi miravano alla vulnerabilità dei dipendenti e hanno cercato di simulare un'attività legittima mentre rubavano tranquillamente quanto più denaro possibile nel minor tempo possibile, durante una sorta di "saccheggio digitale". Apparentemente, le minacce quotidiane, come phishing e siti web pericolosi, possono portare conseguenze molto più gravi della perdita di produttività.

Minacce simili sono in costante evoluzione. Per affrontarle, la cybersecurity deve essere altrettanto agile. L'accesso alla più recente threat intelligence assistita dal cloud aiuta le aziende a stare al passo con i cambiamenti, mentre il machine learning combinato all'esperienza umana garantisce previsione, prevenzione e rilevamento delle minacce rapidi.

DISPOSITIVI MOBILI O OBIETTIVI IN MOVIMENTO?

L'ascesa dei servizi bancari mobili non si ferma ed è una buona notizia per le banche che desiderano offrire nuovi servizi e flessibilità, oltre ad attirare la prossima generazione di clienti. Mentre il 53% di tutti gli utenti di smartphone degli Stati Uniti con un conto bancario utilizza i servizi bancari online[8], questa cifra arriva a quasi il 70% tra gli utenti della nuova generazione.

47%

dei clienti bancari utilizza i servizi bancari mobili.

42%

delle banche si aspetta che i servizi bancari mobili diventino la principale forma di interazione con il cliente nell'arco di tre anni.[9]

Con un mercato di pagamenti mobili stimato sui 27 miliardi di dollari nel 2016[10], non sorprende che i cybercriminali desiderino sfruttare qualsiasi vulnerabilità del mondo mobile. Sfortunatamente per i fornitori di servizi, parte del problema sono gli stessi clienti che attirano i cybercriminali tramite le applicazioni mobili: solo il 53% degli utenti ha software di sicurezza installati sul proprio smartphone e il 57% sul proprio tablet.[11] E anche i cybercriminali ne sono a conoscenza...

Seguendo la tendenza verso l'utilizzo di dispositivi mobili, i cybercriminali stanno tracciando il comportamento degli utenti e passando dal prendere di mira siti web bancari a simulare applicazioni bancarie mobili.[12]

CHI È IL MITTENTE?

Data la bassa adozione di soluzioni di sicurezza per i dispositivi mobili,da parte dei clienti, è fondamentale che le organizzazioni finanziare la includano direttamente nelle loro applicazioni mobili. Tali dispositivi infetti rappresentano un notevole rischio per il settore bancario: malware come Zitmo possono silenziosamente intercettare i messaggi SMS e approvare transazioni avviate dai criminali, di fatto ignorando la comune tecnica di autenticazione a due fattori che prevede l'invio di codici di verifica ai telefoni. Altri tipi di malware, come Wroba, sono in grado di rimuovere applicazioni bancarie legittime dal dispositivo dell'utente e sostituirle con versioni false che sottraggono credenziali e denaro.

Ancora una volta, i fornitori di servizi finanziari si trovano ad affrontare la sfida di scoprire chi c'è all'altro capo del dispositivo: un cliente o un cybercriminale? Questi pagamenti mobili sono autentici? Chi è il mittente? Come puoi proteggere le transazioni se non sai chi le sta conducendo?

59%

delle banche si aspetta che le frodi finanziarie aumentino nei prossimi tre anni.[13]

[8] US Federal Reserve Consumer and Mobile Financial Services 2016

[9] Kaspersky Lab: nuove tecnologie, nuove cyberminacce, analisi dello stato di sicurezza IT nel settore finanziario 2017 (New Technologies, New Cyberthreats, analyzing the state of IT Security in the financial sector 2017)

[10] eMarketer: Negli Stati Uniti i pagamenti mobili triplicheranno nel 2016 (Mobile Payments will Triple in the US in 2016)

[11] Sondaggio sui rischi della sicurezza dei consumatori condotto nel 2016 da Kaspersky Lab

[12] Kaspersky Lab, statistiche delle minacce nel 2016

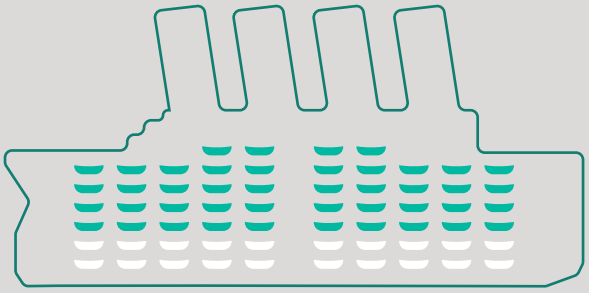
[13] Kaspersky Lab: nuove tecnologie, nuove cyberminacce, analisi dello stato di sicurezza IT nel settore finanziario 2017 (New Technologies, New Cyberthreats, analyzing the state of IT Security in the financial sector 2017)

COME DISTINGUERE LA REALTÀ DALLA FINZIONE

L'attività di separare i veri clienti e transazioni da quelli falsi porta i suoi problemi aggiuntivi: il numero di transazioni esaminate per frode può essere di decine di migliaia al giorno, o addirittura milioni, se prendiamo ad esempio il caso della famosa violazione a Target[14]. Nel caso di Target, gli elevati volumi di avvisi generati da un sistema di sicurezza sono stati presi per falsi positivi e non come tentativo di sottrazione dei dettagli di 70 milioni di carte di credito e altre informazioni dei clienti. Ma basta anche solo che un avviso riesca a infiltrarsi perché si crei scompiglio. I sistemi di sicurezza tradizionali eseguono la scansione in cerca degli stessi comportamenti e delle stesse caratteristiche di transazione che i criminali hanno imparato a simulare.

I requisiti minimi non bastano

Numero delle scialuppe di salvataggio del Titanic



20/64

SCIALUPPE DI SALVATAGGIO A BORDO/ CAPACITÀ EFFETTIVA DELLA SCIALUPPA DI SALVATAGGIO

Le risorse che possono sembrare sufficienti durante una verifica in un giorno specifico, potrebbero non resistere alla prova sotto stress di un incidente reale. Ad esempio, il Titanic salpò con 20 scialuppe di salvataggio a bordo, il minimo legale richiesto. La sua capacità effettiva era di 64 scialuppe, in grado di trasportare 3.547 persone. Sulla nave erano presenti 2.224 i passeggeri. Le scialuppe di cui era provvista la nave permettevano di portare in salvo solo 1.178 persone.

Riconoscere di non essere in grado di bloccare qualsiasi attacco è una cosa, capire il modo in cui affrontare la questione è un'altra. La cybersecurity facile da gestire che combina machine learning e threat intelligence basata su grandi volumi di dati può consentire ai fornitori di servizi finanziari di ottenere la flessibilità di cui hanno bisogno per adattarsi alle minacce e alle tecniche mutevoli ed evolvere con esse. La threat intelligence assistita dal cloud raccolta da milioni di sistemi reali fornisce il tipo di intelligence sulle cyberminacce necessaria per ridurre al minimo le minacce.

Gli alti volumi di falsi positivi possono mettere eccessivamente a dura prova le risorse e lo sforzo derivante dagli avvisi può rivelarsi una minaccia alla pari di qualsiasi altro attacco. La tradizionale sicurezza reattiva non dispone della precisione necessaria per affrontare le odierne minacce sofisticate in continua evoluzione. Non è in grado di distinguere le minacce vere da quelle potenziali in modo efficace. In definitiva, il modo migliore per affrontare questa situazione è tramite il rilevamento multilivello proattivo che unisce analisi euristica, basata sui comportamenti, a treath intelligence, competenza umana e funzionalità antifrode complete.

Non permettere al cybercrimine e alla frode di diventare un "costo aziendale". Combatti e conquista la fiducia dei clienti proteggendo l'autenticità delle transazioni aziendali e dei clienti. Ecco come Kaspersky True CyberSecurity può aiutarti.

70%

delle banche è stato colpito da frode.

$ 1.446

la perdita media per incidente per frode finanziaria su un consumatore.

$ 10.312

è il costo per i clienti aziendali.[15]

[14] Scoprite di più sulla violazione subita da Target qui.

[15] Kaspersky Lab: nuove tecnologie, nuove cyberminacce, analisi dello stato di sicurezza IT nel settore finanziario 2017 (New Technologies, New Cyberthreats, analyzing the state of IT Security in the financial sector 2017)

TRUE CYBERSECURITY. DOVE IL MACHINE LEARNING INCONTRA LA COMPETENZA UMANA

I clienti ritengono che spetti ai fornitori di servizi finanziari proteggerli dalle frodi e dalle violazioni dei dati. Normative quali PCI DSS richiedono ai fornitori di servizi finanziari di utilizzare, tra le altre cose, anti-malware aggiornati. Ma soddisfare solamente i requisiti minimi non è più sufficiente. Non è possibile controllare i contenuti che i clienti scaricano o le attività che eseguono attraverso i propri PC o i propri dispositivi smart. Però si può capire il modo in cui l'azienda si difende dagli attacchi e come vi risponde.

POTETE ADOTTARE UN APPROCCIO PROATTIVO ALLA CYBERSECURITY: TRUE CYBERSECURITY.

Come abbiamo appena visto, gli attacchi informatici sono una realtà. In un mondo dove non è possibile bloccare tutti i pericoli, il modo in cui la tua azienda risponde agli attacchi è importante quanto prevenirli e rilevarli. Kaspersky Lab definisce True Cybersecurity questo approccio flessibile e proattivo. Alla sua base vi è la consapevolezza che nel nostro mondo digitale l'obiettivo fondamentale della cybersecurity è stabilire l'autenticità. E la chiave per raggiungere tale obiettivo è una soluzione di cybersecurity che non intralci l'attività aziendale o aggiunga complessità alla gestione. La facilità d'uso è la potenza della tecnologia.

> La True Cybersecurity non solo è in grado di prevenire, ma anche di rilevare e rispondere agli attacchi informatici in modo rapido e sicuro.

Adottando un approccio alla cybersecurity flessibile e proattivo, i servizi finanziari possono garantire che i Trojan, gli attacchi malware e le minacce mobili e web che devono affrontare i clienti non diventino un problema nelle loro reti aziendali. L'accesso non controllato a dispositivi e web e l'uso di dispositivi USB minacciano tutte le aziende con rischi di tempi di inattività o alla protezione dei dati che comporteranno la perdita di clienti e danni alla reputazione.

Le soluzioni Kaspersky Lab combinano le migliori competenze umane e di intelligence, gli algoritmi di machine learning, l'analisi basata su grandi volumi di dati e la threat intelligence in tempo reale per fornire un reale portfolio Next Generation di soluzioni di cybersecurity.

L'APPROCCIO KASPERSKY LAB CYBERSECURITY È SUPPORTATO DA:

Kaspersky Endpoint Security for Business: Una piattaforma per la sicurezza degli endpoint Next Generation, basata sulla nostra rete di intelligence globale su cloud, Kaspersky Security Network. Combina la treath intelligence basata su grandi volumi di dati, il machine learning e 20 anni di competenza umana per fornire non solo tecniche di prevenzione, ma anche capacità di previsione, rilevamento e risposta con sfide di gestione minime. Scalabile e semplice da usare, Kaspersky Endpoint Security for Business offre protezione multilivello contro minacce note, sconosciute e avanzate, il tutto gestito da un'unica console integrata, che include:

Web, Device e Application Controls che riducono sensibilmente il rischio di attacchi zero-day, software non autorizzato e l'uso improprio di dispositivi, ad esempio USB, spesso i colpevoli principali delle violazioni di dati causate dai clienti. I controlli dei siti web identificano e bloccano i siti nocivi, mentre i controlli di file e applicazioni bloccano l'avvio di programmi non desiderati o non sicuri, riducendo al minimo il rischio per l'utente finale.

Tecnologia AEP (Automatic Exploit Prevention) che tratta e identifica in modo proattivo le minacce sconosciute e avanzate e ne previene il lancio.

Crittografia dei dati che impedisce l'accesso non autorizzato ai file in caso di furto o smarrimento del dispositivo o in seguito a un attacco malware finalizzato al furto di dati. La crittografia è la chiave di volta delle best practice relative alla protezione dei dati globale ed è prevista come tale da molti enti statali.

Gestione dei sistemi che consente attività di gestione, monitoraggio e controllo della sicurezza degli endpoint, della valutazione delle vulnerabilità, delle implementazioni di patch e molto altro, da una singola console centralizzata. Questo consente di semplificare i servizi bancari fondamentali, eseguire le operazioni in modo ininterrotto e sicuro, garantire la soddisfazione dei clienti e aumentare l'efficienza delle risorse.

Sicurezza e gestione dei dispositivi mobili che, tra gli altri elementi, garantisce la sicurezza, anche per i dispositivi di proprietà dei dipendenti, tramite l'applicazione dell'installazione anti-malware, le tecnologie sicure di antifurto e containerization dei dati aziendali/sensibili.

Soluzioni Kaspersky Targeted Security che forniscono ulteriori livelli di sicurezza, esattamente dove sono necessari:

Security for Mail Server che protegge i server Exchange, Linux e Lotus Domino da posta nociva, perdita di dati e spam.

Security for File Server per Windows e Linux che offre protezione centralizzata in tempo reale con impostazioni di configurazione avanzate.

Security for Internet Gateway che garantisce la protezione e il controllo dell'accesso dei dipendenti a Internet.

Security for Collaboration che assicura ai dipendenti la possibilità di condividere informazioni e servizi vitali, ma non malware o altri rischi.

Security for Virtualization che consente ai fornitori di servizi finanziari di sfruttare in modo sicuro tutti i vantaggi derivanti dalla virtualizzazione senza gravare ulteriormente sulle risorse.

Kaspersky DDoS Protection che protegge dagli attacchi di elevata intensità che prendono di mira i sevizi o causano interruzioni gravi.

RENDI LA TRUE CYBERSECURITY UN VANTAGGIO AZIENDALE

I servizi finanziari si basano su elementi quali fiducia, riservatezza e autenticità. La True Cybersecurity consente alle aziende di tenere fede alle promesse proteggendo proattivamente le interazioni con i clienti e le operazioni aziendali.

L'analisi della "catena della criminalità informatica" mostra che gli utenti malintenzionati devono superare ogni punto della catena per raggiungere il loro obiettivo: una sola mitigazione distruggerebbe sia la catena che l'utente malintenzionato.[16]

Rendi la True Cybersecurity un vantaggio aziendale e integrala come parte della strategia generale per sviluppare nuovi prodotti e nuovi servizi, senza compromettere la sicurezza. Utilizza la threat intelligence assistita dal cloud e il machine learning di Kaspersky Lab per fornire più livelli di sicurezza che permetteranno all'azienda di incoraggiare i clienti a utilizzare i servizi self-service, mobili e altre opzioni innovative.

Non permettere al cybercrimine e alla frode di diventare un "costo aziendale". Grazie a una strategia proattiva potrai conquistare la fiducia dei clienti e soddisfare le normative sulla protezione dei dati. Un buon affare inizia dalla conoscenza del cliente, la True Cybersecurity garantisce che ciò avvenga, indipendentemente dal modo in cui tale cliente sceglierà di interagire con te.

True Cybersecurity. Dove il machine learning incontra la competenza umana. Solo con Kaspersky Lab.

SCARICA UNA VERSIONE DI PROVA GRATUITA

Sito web globale di Kaspersky Lab

Blog B2B di Kaspersky Lab