Akamai

WHITE PAPER

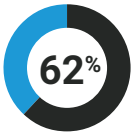
Le piccole e medie imprese devono affrontare attacchi di grande portata

Introduzione

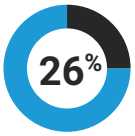
Gli attacchi informatici alle grandi aziende fanno notizia, ma anche le piccole e medie imprese (PMI) si trovano a dover affrontare sempre più gli stessi rischi legati alla sicurezza informatica, al pari delle aziende di maggiori dimensioni. Molti degli exploit di oggi non fanno discriminazioni, perché gli autori degli attacchi si preoccupano solo del loro tornaconto finanziario. Non importa quanto sia grande un'azienda, ma quanto ci si può guadagnare in termini economici. I criminali utilizzano una varietà di metodi per colpire i lavoratori e i dispositivi da cui dipendono, inclusi i dispositivi intelligenti connessi più usati. I provider di servizi Internet sono ben posizionati per aiutare le PMI a difendersi.

Questo breve documento descrive alcune delle minacce più comuni a cui sono esposte le PMI e il loro impatto.

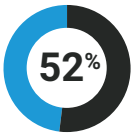
Il sondaggio su tecnologia e piccole imprese pubblicato dalla National Small Business Association ha rivelato alcune interessanti statistiche:



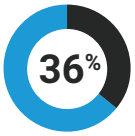
Per il 62% degli imprenditori la sicurezza informatica è una questione molto importante, per un ulteriore 33% è alquanto importante e per il 5% non è affatto importante



Solo il 26% degli imprenditori ha dichiarato di sapere come gestire i problemi legati alla sicurezza informatica



Il 52% degli imprenditori è molto preoccupato che la propria azienda possa essere colpita da un attacco informatico, il 44% è alquanto preoccupato e il 35% ha affermato di aver subito un attacco informatico



Di questi, il 36% ha affermato che sono state inviate informazioni false dai loro domini o indirizzi e-mail, il 5% che sono state rubate informazioni sensibili, il 4% che è stato effettuato l'accesso a conti bancari e il 52% ha segnalato che un attacco ha provocato un'interruzione di servizio

Oggi, è possibile classificare le minacce basate sul web in due macroaree: malware e phishing. Le botnet sono un importante sottoinsieme di malware che merita una speciale attenzione.

Il malware è un software dannoso che viene installato di nascosto sui dispositivi. I siti compromessi possono sfruttare le vulnerabilità dei software presenti su un dispositivo per caricare il malware. Inoltre, gli utenti possono essere indotti ad accedere a un sito web dannoso e a fare clic per caricare un file corrotto. Alcuni malware possono attivarsi su un dispositivo per poi autopropagarsi nell'intera rete. Sono diversi i tipi di malware che prendono di mira le aziende:

I **miner di criptovalute** sono programmi che usano la potenza di elaborazione di un dispositivo senza il consenso della vittima. Comportano una violazione delle risorse delle PMI e sono difficili da individuare perché, a differenza di quanto accade con i ransomware, ai proprietari dei dispositivi non viene chiesto alcun pagamento in denaro.

I **malware specializzati** che vengono caricati sui PoS acquisiscono i dati delle carte di credito e le caricano su un sito antagonista, rendendo vulnerabili gli imprenditori.

Le **minacce persistenti avanzate (APT)** ottengono l'accesso alle reti ed raccolgono dati importanti. Le APT sono progettate per risultare estremamente silenziose in modo da restare attive per periodi di tempo prolungati. Le PMI potrebbero perdere dati di valore oppure, cosa più importante, la fiducia dei clienti o, ancora, possono essere oggetto di azioni normative nel caso di una divulgazione dei dati personali.

I **ransomware** bloccano l'accesso ai file crittografando tutti i contenuti presenti su un dispositivo o un server. Gli autori degli attacchi offrono la chiave di decodifica a un costo significativo, sebbene, in alcuni casi, il pagamento venga riscosso senza inviare la chiave. Nei migliori dei casi, le PMI perdono solo denaro, nel peggiore dei casi, perdono denaro e dati business-critical.

Sono diversi i modi con cui i malware acquisiscono dati di valore. Gli **spyware** cercano dati quali credenziali di accesso e dati finanziari e li comunicano ai criminali. Un malware di **esfiltrazione dei dati** viene creato appositamente per individuare, identificare ed estrarre dati importanti dai computer. I **keylogger** registrano le sequenze di tasti e possono essere addestrati per consentire ai criminali di accedere a conti finanziari, credenziali di accesso ai social media o altre informazioni importanti. I **trojan bancari** monitorano il comportamento degli utenti per apprendere le credenziali di accesso e/o impersonare siti web bancari per rubare denaro.

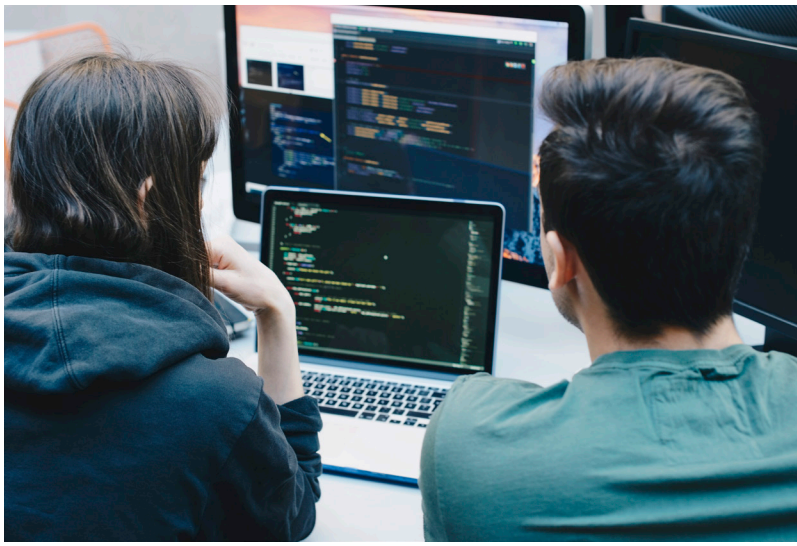
Le **botnet** sono reti di dispositivi infettati dallo stesso malware che vengono controllate tramite un canale centrale (denominato Command and Control [C2]) da un criminale o un gruppo comune. Le botnet sono spesso disponibili per il noleggio e la maggior parte di esse può eseguire molte diverse funzioni per generare denaro, come quelle descritte in precedenza.

Il **phishing** utilizza l'inganno, in particolar modo il social engineering, per indurre le vittime a divulgare informazioni che possono essere monetizzate dall'autore dell'attacco. In passato, gli attacchi di phishing persuadevano gli utenti a fare clic sui link presenti nella posta indesiderata e a divulgare informazioni sensibili. Gli autori degli attacchi di phishing hanno diversificato sostanzialmente i loro sforzi: ora integrano gli URL di phishing anche nei post o nei commenti sui social media, in messaggi di testo, SMS, Skype, Messenger o altri servizi.

I dispositivi mobili sono i principali bersagli del phishing perché, a causa degli schermi di piccole dimensioni e del fatto di svolgere diverse attività insieme, gli utenti potrebbero non notare gli indizi subdoli che fanno capire quando un link è dannoso. Per rendere le cose ancora più difficili, i truffatori usano caratteri molto simili tra quelli disponibili per mimare i nomi dei domini legittimi.

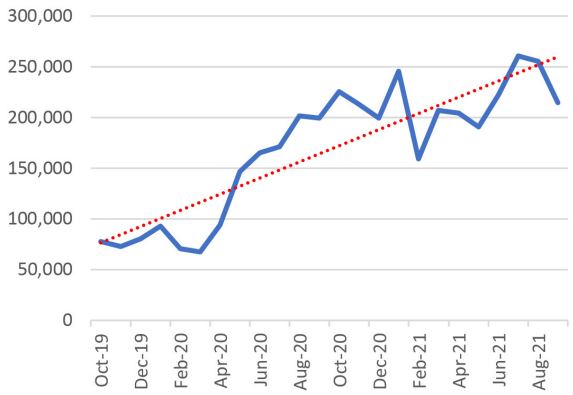
Di seguito sono indicati esempi reali di stringhe di caratteri usati:

7eleven.com
Adîdas.com
adidąs.com
philippineairlınes.com
rolex.com
singaporeair.com
thaiairways.com



Gli attacchi di phishing sono attualmente una tendenza in crescita. Il rapporto sulle tendenze delle attività di phishing relativo al terzo trimestre del 2021 e pubblicato dal gruppo di lavoro anti-phishing afferma: "Il phishing ha raggiunto il record mensile nel terzo trimestre: gli attacchi sono raddoppiati dalla fine del 2019". Il seguente grafico tratto dal rapporto illustra questa tendenza. È molto più facile indurre un utente a svolgere un'azione non intenzionale piuttosto che sfruttare le vulnerabilità di un software.

Gli attacchi di phishing dal quarto trimestre 2019 al terzo trimestre 2021



Anche i dati raccolti dall'operatore e dai team addetti alla ricerca sulla sicurezza aziendale di Akamai mostrano che il ciclo di vita dei nomi di dominio usati per il phishing sta diminuendo, con un calo di circa 1,5 ore nel marzo 2019. Questo aspetto influisce direttamente sulla protezione: i sistemi di difesa devono essere agili quanto gli attacchi.

Conclusione

Questo elenco non comprende tutte le minacce web. Gli autori di attacchi valutano costantemente la fattibilità dei loro exploit e li modernizzano per ottimizzare la resa, facendo cambiare volto e funzioni al loro lavoro. Esistono, poi, altri tipi di malware che sono principalmente una fonte di distrazione o fastidio in quanto mostrano annunci pubblicitari o contenuti indesiderati.

Le PMI devono essere protette dalle minacce provenienti dal web con soluzioni compatibili con le loro specifiche esigenze nel rispetto dei vincoli prefissati. Akamai offre i servizi Secure Internet Access progettati per le PMI per proteggerle dai tipi di attacchi descritti in questo documento, senza alcun onere di gestione. Tutti i dispositivi e le persone presenti in un posto di lavoro, inclusi gli ospiti, vengono protetti automaticamente. I manager aziendali dispongono di un semplice portale grafico su cui possono visualizzare immediatamente ciò che accade sulla loro rete e quali minacce sono state evitate.

I servizi Akamai Secure Internet Access sono realizzati appositamente per aiutare le PMI a:

- Generare ricavi con sistemi di difesa di livello aziendale per le PMI
- Andare oltre la velocità e l'affidabilità e diversificare i servizi per le PMI in base alla sicurezza
- Minimizzare gli ostacoli all'implementazione, ridurre i costi e semplificare la delivery dei servizi con una versione dei servizi Secure Internet Access basata sul cloud

È possibile personalizzare completamente il servizio con un aspetto allineato al brand, insieme al set di funzioni e all'intelligence delle minacce, per adattarsi ai requisiti del mercato locale.

**Tutte le persone. Tutti i dispositivi. In qualsiasi momento.
È qui che entra in gioco Akamai.**

Contattate Akamai oggi stesso per saperne di più.

Akamai potenzia e protegge la vita online. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Con la piattaforma di computing più distribuita al mondo, dal cloud all'edge, siamo in grado di semplificare lo sviluppo e l'esecuzione di applicazioni per i nostri clienti, avvicinando le experience agli utenti e allontanando le minacce. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 06/22.