ANALISI RIASSUNTIVA

Il phishing nel settore finanziario

[stato di internet] - security
volume 7, numero 2

Analisi riassuntiva

Siamo nuovamente giunti al lancio di un altro rapporto sullo stato di Internet - Security per il 2021. Pur potendo accedere ad alcuni dei più vasti database sulla sicurezza al mondo, la visuale di Akamai è limitata al traffico che attraversa le sue reti e viene rilevato dai suoi strumenti.

Per questo rapporto incentrato sul settore dei servizi finanziari, Akamai ha collaborato con la società di intelligence sulle minacce WMC Global. I ricercatori di WMC Global sono esperti nel rilevamento del phishing sferrato tramite SMS (smishing) e dei toolkit sviluppati dai criminali per perpetrare i loro attacchi. Akamai ha stilato il presente rapporto nell'intento di fornire un'ampia visione del panorama delle minacce insieme ad un'analisi approfondita di una specifica minaccia.

Nel 2020, si sono verificati 193 miliardi di attacchi di credential stuffing a livello globale, di cui 3,4 miliardi nel settore dei servizi finanziari con una crescita del 45% rispetto al 2019.

Gli attacchi web sferrati contro il settore dei servizi finanziari hanno rappresentato il 12% degli attacchi globali registrati nel 2020. Akamai ha registrato 736.071.428 attacchi web sferrati contro il settore dei servizi finanziari nel 2020. Il principale tipo di attacco web rivolto contro i servizi finanziari è stato rappresentato dall'attacco LFI (Local File Inclusion) (52%), seguito dagli attacchi SQL injection (33%) e Cross-Site Scripting (9%).

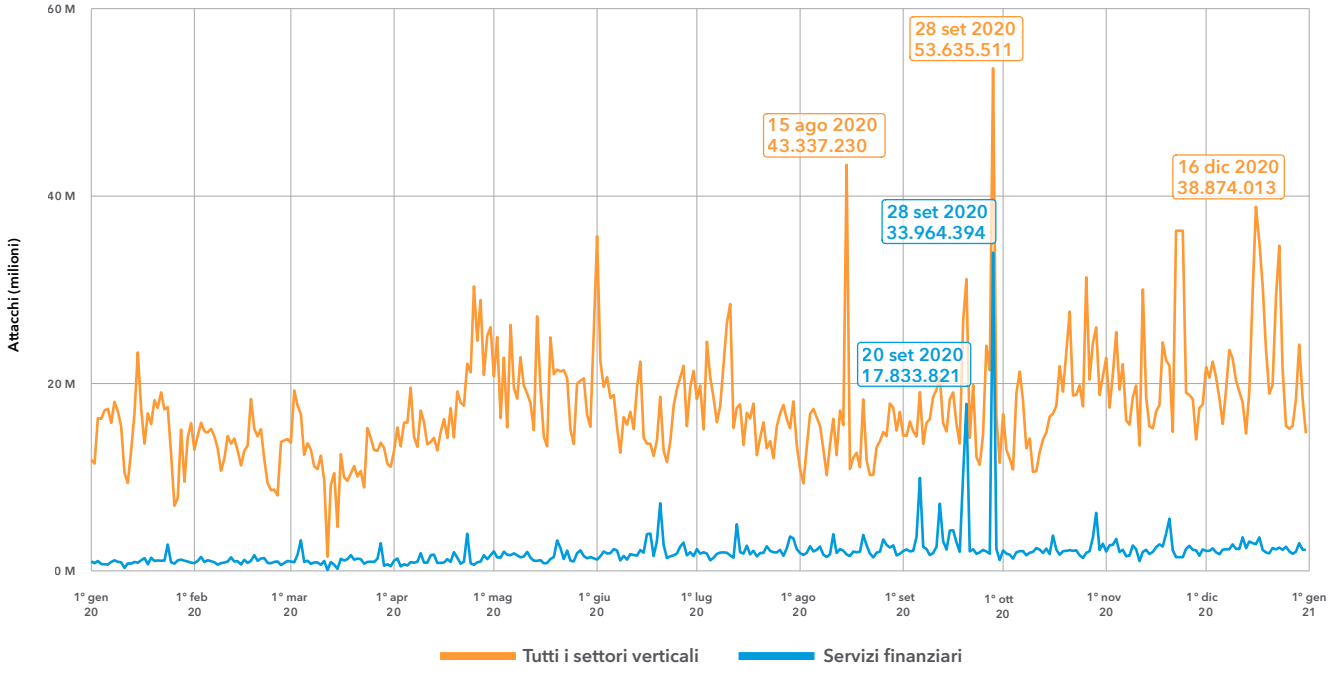
Come risulta nel rapporto, il kit di phishing Kr3pto, che prende di mira gli istituti finanziari e i relativi clienti tramite SMS, ha effettuato lo spoofing di 11 brand nel Regno Unito in oltre 8.000 domini a partire da maggio 2020. Akamai e WMC Global hanno monitorato le campagne di attacchi Kr3pto su più di 80 host diversi (ASN), incluso un host di oltre 6.000 domini Kr3pto.

Nel rapporto, Ian Matthews, CEO di WMC Global, spiega i motivi per cui il phishing effettuato tramite SMS risulta particolarmente efficace.

> Perché il phishing tramite SMS è così efficace? I messaggi SMS vengono usati ovunque nelle comunicazioni odierne, che avvengono perlopiù tramite gli smartphone. Ogni giorno, vengono inviati dai cellulari miliardi di messaggi SMS, che gli utenti aprono rapidamente e frequentemente con una **percentuale rilevata del 98%**.

Ian Matthews
CEO di WMC Global

Attacchi giornalieri alle applicazioni web
1° gennaio 2020 - 31 dicembre 2020



Il numero di attacchi basati sul web e alle applicazioni è rimasto elevato nel 2020 né sembra destinato a rallentare in tempi brevi. Akamai ha registrato 6.287.291.470 attacchi web a livello globale, di cui 736.071.428 sferrati solo contro il settore dei servizi finanziari.

Anche gli attacchi DDoS sono aumentati del 15% nel 2020 rispetto al numero di attacchi sferrati nell'anno precedente contro il settore dei servizi finanziari. Negli ultimi tre anni (2018-2020), gli attacchi DDoS sferrati contro il settore dei servizi finanziari sono aumentati del 93% a indicare che l'interruzione sistemica rimane sempre un'opzione per i criminali, che prendono di mira le applicazioni e i servizi richiesti per le attività quotidiane.

Una minaccia costante e globale

In questo rapporto, viene presentata una ricerca condotta sugli autori delle minacce e sui kit di phishing utilizzati per prendere di mira il settore dei servizi finanziari o i suoi utenti. Il settore dei servizi finanziari nel Regno Unito è stato di recente minacciato da un autore di attacchi relativamente nuovo che ha sviluppato kit di phishing dinamici in grado di eludere in modo efficace metodi di autenticazione secondari.

Il concetto di PhaaS (Phishing-as-a-Service) esiste da qualche anno: alcuni sviluppatori di siti web esperti creano kit di phishing complessi, che, talvolta, sono repliche quasi identiche del brand o dell'istituto finanziario preso di mira. Questi kit sono completi di funzionalità e supporto operativo back-end, pertanto lo sviluppatore deve solo vendere i kit creati a criminali meno esperti che, a loro volta, potranno utilizzarli contro gli utenti.

Kr3pto ha attirato l'attenzione di WMC Global e Akamai dopo aver sferrato i suoi kit di phishing contro 11 diverse banche nel Regno Unito. Considerando la portata e il rapido avanzamento degli attacchi sferrati contro le banche, entrambe le società erano ansiose di indagare sulla loro origine.

Questo kit di phishing prende di mira i nomi utente e le password delle sue vittime, nonché qualsiasi metodo di autenticazione secondario utilizzato, come domande/risposte di sicurezza e PIN inviati tramite SMS. Il workflow utilizzato da questi kit è agile e si adatta dinamicamente all'experience della vittima quando accede alla propria banca.

Kr3pto inizia l'attacco inviando alla vittima "un'esca" tramite un messaggio SMS, in cui segnala un account bloccato o la configurazione di un nuovo beneficiario. Tra il 12 gennaio e il 12 febbraio 2021, WMC Global ha monitorato più di 4.000 campagne collegate al kit Kr3pto che sono state effettuate tramite SMS. Le "esche" vengono inviate tramite SMS per "offuscare" le finalità degli attacchi. La maggior parte dei reparti operativi aziendali, così come le soluzioni per la sicurezza degli endpoint domestici e gli account e-mail generici, impediscono alle e-mail dannose di raggiungere la posta in arrivo della vittima. Questi sistemi di protezione non sono perfetti, ma evitano il verificarsi della maggior parte degli attacchi. Ecco perché i criminali sono passati all'utilizzo degli SMS e, persino, dei social media per inviare le loro "esche".

I kit dinamici come Kr3pto cercano di sfruttare la mancanza di potenti opzioni 2FA, non solo nel settore dei servizi finanziari, ma a livello globale. Il processo utilizzato dal kit Kr3pto per raggiungere questo obiettivo non è nuovo, ma la sua ampia diffusione implica il rischio che possa diventare una pratica comune nel prossimo futuro. Gli istituti finanziari, così come altri importanti brand di consumo, devono adottare alternative 2FA/MFA più potenti per la protezione e la mitigazione di questi attacchi.

In questo rapporto, viene esaminato anche un kit di phishing aziendale noto come Ex-Robotos. I kit di phishing che prendono di mira gli account aziendali comportano un rischio particolarmente elevato, perché creano un'esposizione maggiore rispetto alla vittima presa di mira. Le credenziali compromesse dai kit di phishing aziendali rendono immediatamente vulnerabile l'account in questione, come il sistema della posta elettronica dell'ufficio o l'archivio dei documenti.

Kr3pto inizia l'attacco inviando alla vittima "un'esca" tramite un messaggio SMS, in cui segnala un account bloccato o la configurazione di un nuovo beneficiario. **Tra il 12 gennaio e il 12 febbraio 2021, WMC Global ha monitorato più di 4.000 campagne collegate al kit Kr3pto che sono state effettuate tramite SMS.**

Secondo i dati registrati dall'Akamai Intelligent Edge Platform, si sono verificati più di 220.000 accessi all'indirizzo IP API utilizzato per Ex-Robotos nell'arco di 43 giorni. In effetti, il traffico verso questo indirizzo ha colpito, in media, decine di migliaia di vittime al giorno tra il 31 gennaio e il 5 febbraio 2021.

Esaminando i registri relativi al kit Ex-Robotos, WMC Global ha rilevato una vasta campagna di attacchi sferrati per compromettere le credenziali, spesso da parte di gruppi di criminali online, che cercano di "inondare" un sito web di phishing con nomi utente/password fittizi nel tentativo di indebolire i registri con queste informazioni e rendendo quasi impossibile per l'autore della minaccia elaborare tutti i dati per individuare vittime reali.

I kit di phishing come Ex-Robotos e Kr3pto sono solo la punta dell'iceberg: centinaia di kit vengono sviluppati e distribuiti ogni giorno. Gli attacchi sono implacabili: l'economia del phishing nel suo complesso è cresciuta in modo esponenziale su base annua, poiché gli sviluppatori sfruttano le stesse tecnologie e le medesime tecniche web che consentono alle aziende di rimanere agili e aggiornate.

Si sono verificati più di **220.000 accessi all'indirizzo IP API utilizzato per Ex-Robotos** nell'arco di 43 giorni.

Per un'analisi approfondita di questa ricerca, è possibile scaricare la versione integrale del rapporto sullo stato di Internet - Security:

Il phishing nel settore finanziario

Visitate il sito web https://www.akamai.com/soti

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand mondiali si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 05/21.