OUCH! | Gennaio 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Il Social Engineering

Introduzione

Una delle impressioni errate che molte persone hanno dei criminali informatici è credere che utilizzino unicamente strumenti molto avanzati nelle loro attività di hacking. Questo non corrisponde sempre alla verità. Gli hacker sanno che spesso il modo più semplice per rubare le tue informazioni, per entrare nel tuo account o infettare il tuo sistema consiste semplicemente nell'ingannarti in modo da compiere un errore. In questa newsletter imparerai come questi attacchi, basati sul Social Engineering, funzionano e cosa puoi fare per proteggerti.

L'autore di questo numero

James Lyne (**@jameslyne**) è un istruttore SANS certificato nonché Global Head of Research in Sophos. Passa il suo tempo a individuare e analizzare le più recenti e complesse creazioni dei cyber criminali. È anche autore dei corsi Metasploit (SEC580) e Social Engineering (SEC567) del SANS Institute.

Cos'è il Social Engineering

Il Social engineering è un attacco psicologico in cui qualcuno ti inganna per portarti a compiere un'azione che non dovresti compiere. Il concetto del social engineering non è certo una novità: esiste infatti da migliaia di anni e si basa sullo stesso approccio adottato dai truffatori. Ciò che rende la tecnologia molto più efficace è la mancanza di possibilità di vedere chi sta tentando la truffa: un attaccante può facilmente fingere di essere chiunque voglia e mirare a colpire milioni di persone in tutto il mondo. Anche te. Gli attacchi basati sul Social Engineering possono inoltre oltrepassare molte tecnologie di sicurezza. Il modo più semplice per capire come funzionano questi attacchi e proteggerti da essi è di esaminare un paio di esempi reali.

Supponi di ricevere una telefonata da qualcuno che dichiara di lavorare per un'azienda di supporto informatico, o per il tuo fornitore di servizi o per il supporto tecnico Microsoft. La persona spiega che il tuo computer effettua esplorazioni continue della rete, per cui pensa che sia stato infettato. Per questo motivo gli è stato assegnato il compito di aiutarti a renderlo sicuro. La persona spiegherà il problema con dovizia di termini tecnici e cercherà di confonderti illustrandoti una serie di attività complesse per convincerti che il tuo computer è infetto. Ad esempio, ti potrebbe chiedere di controllare la presenza di determinati file suo tuo computer e guidarti nella ricerca. Quando avrai trovato questi file, il chiamante ti assicurerà del fatto che si tratta di prove che il computer è infetto, quando in realtà questi file sono comuni file di sistema presenti in qualsiasi altro computer nel mondo. Una volta che ti avrà ingannato, farà pressione perché tu compra un software di sicurezza o affinché tu gli dia accesso al tuo computer in modo che possa essere sistemato. Il software che ti verrà proposto altro non

Il Social Engineering

è che un programma maligno che, se installato, infetterà il tuo computer. E tu avrai anche pagato per farlo! Se, invece, permetterai l'accesso remoto al tuo computer, i criminali se ne impossesseranno, ruberanno i tuoi dati o lo useranno per i loro loschi traffici.

Il buon senso è la difesa migliore per identificare e bloccare la maggior parte degli attacchi di Social Engineering.

Un altro esempio è un attacco via email chiamato la "Frode dell'amministratore delegato" (CEO Fraud, in inglese) che più spesso ha luogo nelle aziende: un cyber criminale cerca informazioni sulla tua azienda online e individua il nome di un manager o di un collega. L'attaccante crea un email camuffandola come proveniente dalla persona individuata e te la invia. L'email chiede urgentemente di fare qualcosa, come effettuare un pagamento o inviare informazioni confidenziali dell'azienda o degli impiegati. Spesso queste mail fingono che un'emergenza richieda urgentemente che tu scavalchi le procedure di sicurezza standard, chiedendo ad esempio di inviare informazioni altamente sensibili a un account personale su Gmail. Ciò che rende questi attacchi così pericolosi è la ricerca che viene svolta preventivamente dal criminale informatico. Inoltre, le tecnologie di sicurezza come gli anti-virus o i firewall non sono in grado di individuare o bloccare questi attacchi perché non c'è presenza né di malware né di link maligni.

Ricorda: gli attacchi di Social Engineering come questi non sono limitati a chiamate telefoniche o email. Possono avvenire in ogni forma, ad esempio via SMS, strumenti di messaggistica, social network o anche di persona. La chiave è sapere come individuarli: tu sei la tua miglior difesa.

Individuare e bloccare gli attacchi di Social Engineering

Fortunatamente, fermare questi attacchi è più semplice di quanto si pensi. Il buon senso è la tua miglior difesa: se qualcosa sembra sospetto, potrebbe trattarsi di un attacco. Gli indizi più comuni di un attacco di Social Engineering sono i seguenti.

- Si cerca di creare un grande senso di urgenza per convincerti a compiere un errore
- Vengono richieste informazioni a cui non si dovrebbe avere accesso o che dovrebbero già sapere, come ad esempio il tuo numero di conto
- Ti viene richiesta una password: nessuna azienda reale te la chiederà mai

Il Social Engineering

- Viene fatta pressione allo scopo di scavalcare o ignorare le procedure di sicurezza che devi seguire nel tuo lavoro
- Ti viene proposto qualcosa troppo bello per essere vero. Ad esempio, ti viene notificata la vincita a una lotteria, sebbene tu non ne avessi mai sentito parlare
- Ricevi una strana email da un amico o da un collega, scritta in modo diverso da quello normalmente utilizzato da lui. Un criminale informatico potrebbe aver avuto accesso al loro account mail e sta ora tentando di ingannarti. Per proteggerti, verifica la richiesta contattando il tuo amico o il tuo collega usando un mezzo di comunicazione diverso, come il telefono.

Se sospetti che qualcuno stia tentando di ingannarti, non comunicare con lui in alcun modo. Se l'attacco ha a che fare con il tuo lavoro, notificalo al tuo help desk o al dipartimento sicurezza. Ricorda: il buon senso è spesso la tua miglior difesa.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Il Phishing:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf
La truffa del CEO:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_it.pdf
Il Ransomware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley