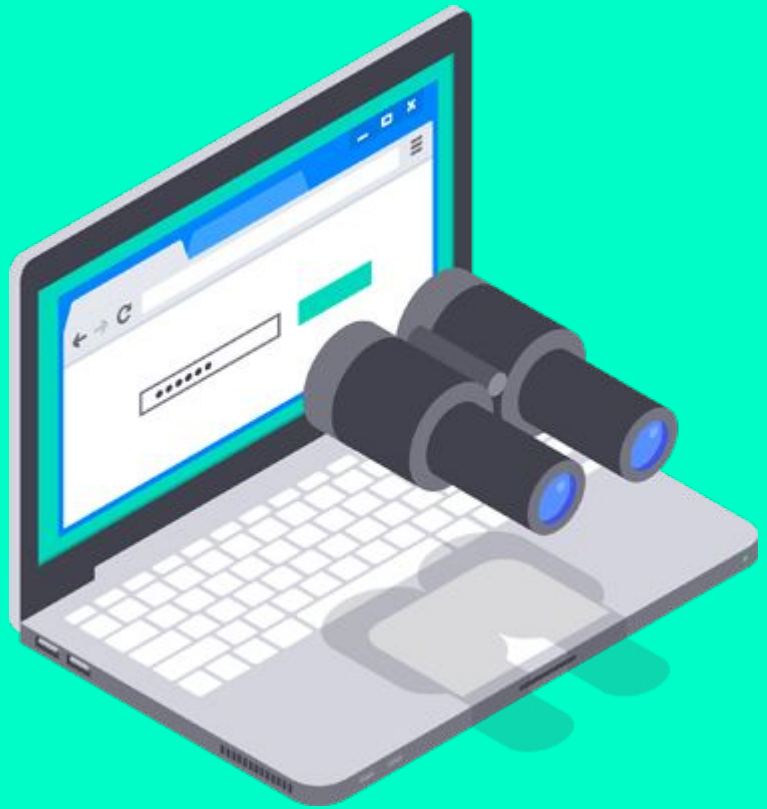
SPYWARE



Che cos'è uno spyware

Uno spyware, in informatica, è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso. In un senso più ampio, il termine è spesso usato per definire un'ampia gamma di malware (software maligni) dalle funzioni più diverse, quali l'invio di pubblicità non richiesta (spam), la modifica della pagina iniziale o della lista dei Preferiti del browser, oppure attività illegali quali la redirezione su falsi siti di commercio elettronico (phishing)

Tipi di spyware

I principali tipi in cui si dividono sono 5

INFOSTEALER

Gli infostealer sono programmi che hanno la capacità di scansionare computer infetti e rubare numerose informazioni personali, tra cui cronologie di navigazione, nomi utente, password, indirizzi e-mail, documenti personali e file multimediali. A seconda del programma, gli infostealer memorizzano i dati che raccolgono su un server remoto o in locale, per recuperarli in seguito.
Nella maggior parte dei casi, gli infostealer sfruttano le carenze di sicurezza dei browser per raccogliere i tuoi dati personali. A volte usano anche i cosiddetti injection script per aggiungere campi ai moduli web. Quando digiti le informazioni richieste e premi “Invia”, le informazioni non vengono recapitate all’amministratore del sito web ma direttamente all’hacker, che potrà quindi utilizzarle per rubarti l’identità su Internet.

PASSWORD STEALER

I password stealer sono molto simili agli infostealer, con la sola differenza che sono pensati specificatamente per rubare le credenziali di accesso dai dispositivi infetti. Rilevati per la prima volta nel 2012, questi spyware non rubano le tue password mentre le digiti: al contrario, si collegano al browser per estrarre tutti i tuoi nomi utente e le relative password; inoltre, possono anche registrare le tue credenziali di accesso al sistema.

I software di sicurezza affidabili sono in grado di rimuovere la maggior parte dei password stealer, ma alcuni tipi riescono comunque ad evitare il rilevamento modificando gli hash dei file prima di ogni attacco. Come con gli infostealer, i creatori di password stealer possono scegliere se memorizzare i dati raccolti su un server remoto o in un file nascosto sul tuo disco rigido.

KEYLOGGER

I keylogger sono programmi spyware che registrano i tasti che digiti sulla tastiera di un computer infetto. Mentre i keylogger basati su hardware registrano ogni sequenza di tasti in tempo reale, i keylogger basati su software raccolgono schermate periodiche delle finestre attive: in questo modo, possono registrare password (se non sono crittografate sullo schermo), dati delle carte di credito, cronologie di ricerca, e-mail e messaggi sui social network, così come la cronologia del browser.
Sebbene siano principalmente usati dagli hacker per raccogliere dati sensibili da vittime ignare, negli ultimi anni i keylogger sono anche impiegati per motivi più pratici: in particolare, alcuni titolari di aziende sfruttano i keylogger per monitorare l'attività dei propri dipendenti, inoltre, anche le forze dell'ordine negli Stati Uniti hanno utilizzato keylogger per arrestare criminali noti e colpire gli spacciatori di droga.

TROJAN BANCARI

I trojan bancari sono programmi pensati per accedere e registrare informazioni sensibili memorizzate su sistemi bancari online (o elaborate tramite essi). I trojan bancari sono generalmente mascherati da software autentici e sono in grado di modificare le pagine web sui siti di home banking, cambiare i valori delle transazioni e persino effettuare trasferimenti bancari a vantaggio degli hacker. Come tutti gli altri tipi di spyware, i trojan bancari includono una backdoor, così possono inviare tutti i dati raccolti a un server remoto.
Generalmente, questi programmi prendono di mira istituzioni finanziarie come banche, agenzie di brokeraggio, servizi finanziari online e servizi di portafoglio elettronico. Generalmente i trojan bancari sono estremamente sofisticati, quindi non vengono rilevati nemmeno dagli avanzatissimi sistemi di sicurezza di alcune istituzioni finanziarie.

MODEM HIJACKER

Con il passaggio graduale dalla connessione analogica alla banda larga nell'ultimo decennio, i modem hijacker sono diventati un ricordo del passato: sono forse gli spyware più datati. Di norma, mostravano pop-up pubblicitari che richiedevano all'utente di cliccare su di essi: in tal caso, gli spyware scaricavano di nascosto un file che avrebbe poi preso il controllo del modem analogico. Una volta preso il controllo del computer, il modem hijacker disconnette la linea telefonica dalla sua connessione locale collegandola invece a una internazionale. Quasi tutti gli hacker possedevano numeri di telefono a tariffa elevata (di solito destinati alle chatline per adulti) registrati in Paesi con leggi sulla criminalità informatica scarse, come Cina, Russia o alcuni Paesi sudamericani. Solitamente le vittime si rendevano conto del problema solo il mese successivo, quando ricevevano una bolletta telefonica astronomica.

PEGASUS

Pegasus è uno dei più famosi e pericolosi spyware in circolazione ed è divenuto celebre per i vari attacchi che ha compiuto nel campo della politica e del giornalismo.

DOVE NASCE

Lo spyware ,che prende il nome dalla figura mitologica greca, è stato prodotto dalla società israeliana NSO, impresa specializzata nel campo delle armi informatiche , o come si definiscono loro: “gruppo specializzato in tecnologie di sorveglianza digitale”, per penetrare la frontiera di un dispositivo elettronico e raccogliere ogni possibile informazione su di esso e sul suo possessore.

COM'È FATTO?

Pegasus è composto da vari componenti tra cui i più rilevanti:

-la PARTE AGENTE
colei che attacca il dispositivo e sottrae i dati dell'utente

-la INTERFACCIA DI COMANDO
interfaccia grafica che permette allo hacker di controllare a distanza il dispositivo vittima permettendogli anche di inviare comandi in backdoor.

-la BACKDOOR
componente che viene installato sul dispositivo e apre un canale di comunicazione con l'operatore ,generalmente via protocollo HTTPS, riceve ed esegue comandi dall'operatore. Generalmente questo componente è completamente invisibile una volta installato.

-il VETTORE DI ATTACCO

la tecnica mediante la quale l'accesso non autorizzato può essere ottenuto da un hacker su un dispositivo o una rete sfruttando le debolezze in termini di sicurezza del dispositivo.
Inoltre il vettore di Pegasus è molto sofisticato dato che è replicato anche all'interno di droni militari e consente allo spyware di nascondersi dai controlli di sicurezza.

FUNZIONAMENTO

Pegasus ,per entrare in un dispositivo, prima di tutto, cerca di conquistare i privilegi di root; come quello amministratore o quelli dei software di amministrazione del dispositivo. Dopodichè infetta tutti i componenti del dispositivo venendo aiutato da uno sviluppatore esterno, cioè contatta l'hacker per richiedere delle componenti per avere sempre più accessi al dispositivo, infatti, una delle peculiarità di Pegasus è quella di essere versatile su tutti i dispositivi perché si basa sul tipo di device, sulla versione del firmware e sul sistema operativo.

Il processo di infezione può durare millisecondi come potrebbe durare anche giorni se non settimane a seconda dell'intervento degli hacker esterni che forniscono componenti allo spyware.

Pegasus attacca ha un metodo di attacco molto intelligente e quasi impossibile da scovare perché esso può rimanere silente sul dispositivo per tempi lunghissimi e compiere piccoli furti di informazioni ogni tanto.

Ciò che ha reso Pegasus particolarmente potente è stato il modo in cui la vittima non aveva bisogno di installarlo o attivarlo accidentalmente. È sufficiente un exploit senza necessità di clic o di azione da parte dell'utente per attivare lo spyware; infatti,per esempio, agli utenti iPhone, è bastato aprire un iMessage per attivare il software malevolo.

EFFETTI

Una volta che un dispositivo è stato infettato da Pegasus, il malware può leggere messaggi ed e-mail, ascoltare chiamate, registrare password e persino tenere traccia delle posizioni visitate. Il primo caso noto di infezione da Pegasus risale al 2016, quando si è installato sull'iPhone di un attivista per i diritti umani.

Nonostante le affermazioni secondo cui Pegasus doveva essere utilizzato solo come mezzo per raccogliere informazioni contro potenziali minacce terroristiche, migliaia di vittime di questo spyware sono state attivisti e giornalisti, il che ha spinto Amnesty International a parlare apertamente.

L'organizzazione afferma che, sebbene il gruppo NSO potrebbe non prendere di mira personalmente le vittime, deve comunque assumersi la responsabilità di come la sua tecnologia venga utilizzata in modo improprio. Soprattutto quando quella tecnologia si trova sui telefoni di importanti funzionari governativi in tutto il mondo.

Solitamente lo spyware attacca i dispositivi mobili e ha attaccato molti giornalisti e azionisti politici ed è nato persino uno spyware molto simile a Pegasus ,creato dall’ azienda macedone CYTROX, nominato Predator; impiegato per vari attacchi informatici a soggetti politici balcani.

Per ulteriori notizie di attacchi spyware e di pegasus clicca qui.

COME DIFENDERSI?

Riavvia ogni giorno il dispositivo. Se il dispositivo viene riavviato ogni giorno, gli aggressori dovranno reinfettarlo più e più volte. Nel tempo, questo aumenta le possibilità di rilevamento; potrebbero essere registrati un arresto anomalo o artefatti che rivelano la natura dell'infezione furtiva.

Mantieni aggiornato il dispositivo

Non cliccare mai sui link ricevuti tramite SMS

Usa sempre una VPN

per ulteriori consigli clicca qui

FONTI INFORMAZIONI

- NORDVPN
- WIRED
- MAGZINE
- WIKIPEDIA