Non ci sono più gli hacker di una volta

Nel variegato mondo delle minacce di sicurezza informatica uno dei pericoli più insidiosi è sicuramente il **Remote Access Trojan (RAT)**.

Si tratta di un programma malware che lavora includendo una back door per il controllo amministrativo del computer bersaglio.

Una delle inside principali è proprio l'abilità del **RAT** di essere scaricato in modo invisibile con un programma richiesto dall'utente – che si tratti di un'applicazione, un gioco o un semplice PDF – o inviato come allegato a un'e-mail.

Una volta che il sistema host è compromesso, l'intruso può usarlo per distribuire RAT ad altri computer vulnerabili e creare una botnet.

Adwind: il più pericoloso

Esistono, come per tutti i malware, vari tipi di RAT, ma non c'è dubbio che il più "completo" sia **Adwind**, grazie alla sua capacità di sottrarre informazioni dai sistemi bersaglio, di crittografare file e di impossessarsi delle credenziali **VPN**.

Come se non bastasse, nelle sue ultime release, è stata aggiunta l'abilità di fare keylogging, screenshot, registrare video dalla webcam del pc bersaglio e audio dal microfono.

Scoperto per la prima volta nel 2012 – al tempo era noto come Frutas – Adwind mantenendo la sua struttura è anche chiamato

AlienSpy, Unrecom, Sockrat, JSocket e **JRAT**. Nel suo primo picco di attività (2013-2016) è stato indicato come il colpevole di quasi 160 campagne di attacco nei confronti di oltre 70mila target.

Tra queste spicca quella portata avanti da AlienSpy sul finire del 2015 che ha preso di mira tutti i maggiori player nel settore della finanza e delle TelCo statunitensi oltre ad alcuni enti governativi attraverso delle campagne di phishing mirate. All'interno delle e-mail incriminate il malware era ben nascosto nei panni di fatture, note spesa o addirittura ordine da parte di fornitori.

La facilità con cui era riuscito a diffondersi era anche in parte dovuta all'abilità del malware di funzionare su tutte le principali piattaforme disponibili sul mercato: da Windows a Mac, passando per Linux e Android.

Bersagli diversificati

Se inizialmente Adwind sembrava avere come bersaglio unicamente i settori citati poco prima, di recente, secondo uno studio pubblicato da un'università americana, il malware è cominciato ad apparire come il principale indiziato in attacchi che hanno coinvolto oltre 1.500 organizzazioni di oltre 100 Paesi; organizzazioni che andavano dal settore dell'industria pesante fino ai piccoli studi legali. Un pattern che non sembra seguire particolari "agende" come spesso accade quando alle spalle di queste campagne ci sono gruppi hacker sponsorizzati. Nel 2017 è comparso dopo una serie di incidenti che hanno coinvolto le principali aziende del settore aerospaziale europeo, preambolato da una attenta strategia di social engineering. Nel 2018 ha sfruttato una vulnerabilità di Autodesk A360 per ottenere il controllo numerosi sistemi. Nel 2019 è stato trovato in oltre 2 milioni di email di phishing.

Il Cyber crimine diventa SaaS

Uno dei motivi per questa apparente randomizzazione degli attacchi è dovuta al fatto che Adwind, nelle sue versioni **JSocket**, è da qualche tempo distribuito nel dark web, in una sorta di perverso e-commerce del Cyber crimine.

I prezzi variano dai 30 dollari per il pacchetto contenente il Malware pronto ad essere lanciato (solo per un mese) fino ai 200 per una licenza illimitata, una sorta di crimine as a service; il tutto – ovviamente – corredato di supporto tecnico e assistenza via mail.

Sfortunatamente il fenomeno non è limitato ai soli RAT: il mercato del Dark web è diventato un vero e proprio retail che opera su piattaforme, non troppo differenti da un qualsiasi e-shop, che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto, il tutto incorniciato con un'interfaccia intuitiva e responsive facilmente navigabile. Non mancano neppure elementi di customer care, come accennato, che comprendono FAQ, chat di supporto e dettagliate pagine di aiuto.

Oltre ai già i citati RAT si possono trovare Decrittatori di Password, campagne di Phishing pre-confezionate, keyloggers e pacchetti completi "end to end" che comprendono tutti gli elementi necessari a compiere frodi bancarie. Naturalmente in questo mondo regnano le cripto valute, per loro natura difficili da tracciare.

Gli esempi qui elencati sono solo la punta dell'iceberg di un mondo che, nonostante i migliori tentativi delle autorità preposte, sembra essere solo in crescita.

Oggi, esistono decine di piattaforme che vendono software come i malware e per ogni sito che viene abbattuto un altro eventualmente prende il suo posto.

È stato stimato che nel 2017 negli Stati Uniti d'America le frodi commesse online hanno causato circa 17 miliardi di dollari di perdite ad aziende e privati, mentre in Europa l'Italia si piazza in seconda posizione per numero di crimini subiti.

È sicuramente utopistico augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono aiutare a scongiurare questi attacchi.

Una delle misure più semplici parte dall'igiene delle password: una password sicura non deve essere scontata, non deve richiamare al tuo nome/data di nascita o a quello dei tuoi cari, non deve essere eccessivamente corta e deve includere caratteri speciali.

Un altro consiglio è quello di utilizzare, laddove possibile, un sistema autenticazione a due fattori, che assicura un'ulteriore barriera di protezione anche nel caso in cui venga sottratta la password.

Sono regole semplici da seguire, ma che possono migliorare drasticamente la resilience dei propri sistemi e dispositivi.

Sparisce la barriera d'ingresso

Ma facendo un passo indietro, la preoccupazione più grande è inerente alla facilità di accesso per attori malintenzionati agli strumenti necessari per compiere crimini on-line.

La scena del Criminal hacking fino a pochi anni fa era stata dominata da un substrato di persone in possesso di un certo livello di *skill*.

La recente ondata di pacchetti e soluzioni *ready made* rischia di inondare il web di aspiranti Criminal hacker che ora non hanno necessariamente le competenze e le conoscenze necessarie per portare avanti campagne di phishing o di malware da soli,

ma che grazie ai servizi del Dark Web si trovano le soluzioni già preconfezionate e pronte ad essere utilizzate.

La democratizzazione del Cyber crime, quindi, sembra essere alle porte.

https://www.key4biz.it/non-ci-sono-piu-gli-hacker-di-una-volta/269783/