Cyber-raccolta si riferisce all'uso di guerra informatica tecniche per condurre spionaggio . Attività di cyber-raccolta in genere si basano su l'inserimento di minacce informatiche in una rete mirata o un computer al fine di cercare, raccogliere e trapelare informazioni sensibili.

Cyber-collezione iniziata nel lontano 1996, quando la diffusione generalizzata di connettività Internet ai sistemi aziendali del governo e preso slancio. Da quel momento, ci sono stati numerosi casi di tale attività.

Oltre agli esempi di stato sponsorizzato, cyber-raccolta è stato utilizzato anche dalla criminalità organizzata per l'identità e il furto di e-banking e dalle spie aziendali. Operazione High Roller usato agenti cyber-raccolta al fine di raccogliere PC e smart-phone informazioni che è stato utilizzato per razziare elettronicamente conti bancari. Il Rocra , alias Red October, sistema di raccolta è un "di spionaggio per il noleggio" operazione da criminali organizzati che vendono le informazioni raccolte al miglior offerente.

Contenuto

Piattaforme e funzionalità

Strumenti Cyber-raccolta sono stati sviluppati da governi e gli interessi privati per quasi ogni sistema operativo del computer e smart-phone. Gli strumenti sono noti per esistere per Microsoft, Apple e computer Linux e iPhone, Android, Blackberry e Windows Phone. I principali produttori di COTS (COTS) tecnologia di raccolta informatica includono Gamma Group dal Regno Unito e Hacking Team in Italia. Bespoke aziende strumento di cyber-raccolta, molti pacchetti offerta COTS di zero-day exploit, includono Endgame, Inc. e Netragard degli Stati Uniti e VUPEN dalla Francia. Le agenzie di intelligence degli Stati hanno spes[illegible]rie squadre per sviluppare strumenti cyber-raccolta,

- *Scansione di dati* : storage locale e la rete vengono analizzati per trovare e copiare i file di interesse, questi sono spesso documenti, fogli di calcolo, file di progettazione come ad esempio file Autocad e file di sistema come il file passwd.
- *Cattura posizione* : GPS, WiFi, reti e altri sensori allegate sono utilizzati per determinare la posizione e il movimento del dispositivo infiltrato
- *Bug* : il microfono del dispositivo può essere attivato al fine di registrare l'audio. Allo stesso modo, flussi audio destinati altoparlanti locali possono essere intercettate a livello di dispositivo e registrati.
- *Nascosti reti private* che ignorano la sicurezza della rete aziendale. Un calcolo che viene spiato può essere collegato a una rete aziendale legittima che è pesante monitorato per l'attività del malware e allo stesso tempo appartiene a una rete WiFi privata al di fuori della rete aziendale che perde informazioni riservate fuori del computer di un dipendente. Un computer di questo tipo è facilmente impostato da un doppio agente che lavora nel reparto IT per installare una seconda scheda wireless in un computer e un software speciale per monitorare a distanza il computer di un dipendente attraverso questa seconda scheda di interfaccia senza che esse siano a conoscenza di una banda laterale canale di comunicazione tirando informazioni fuori del suo computer.
- *Camera* : le telecamere di dispositivi possono essere attivati in modo da catturare di nascosto immagini o video.
- *Keylogger e mouse Logger* : l'agente di malware in grado di catturare ogni tasto, il movimento del mouse e fare clic che l'utente di destinazione fa. In combinazione con afferra schermo, questo può essere utilizzato per ottenere le password che vengono immessi utilizzando una tastiera virtuale sullo schermo.
- *Schermo Grabber* : l'agente di malware può prendere immagini periodici di cattura dello schermo. Oltre a mostrare le informazioni sensibili che non possono essere memorizzati sulla macchina, come ad esempio i saldi di e-banking e web mail criptata, questi possono essere utilizzati in combinazione con i dati chiave e logger mouse per determinare le credenziali di accesso per altre risorse Internet.
- *Crittografia* : raccolti i dati vengono crittografati di solito al momento della cattura e possono essere trasmessi in diretta o conservati per exfiltration tardi. Analogamente, è pratica comune per ogni specifica operazione utilizzare la crittografia specifica e capacità poli-morfico dell'agente cyber-raccolta al fine di garantire che il rilevamento in una posizione non comprometta altri.
- *Crittografia Bypass* : Poiché l'agente di malware opera sul sistema di destinazione con tutti i diritti di accesso e dell'account utente del bersaglio o amministratore di sistema, la crittografia viene bypassato. Ad esempio, l'intercettazione di audio utilizzando il microfono e dispositivi di uscita audio permette il malware catturare entrambi i lati di una chiamata Skype crittografato.
- *Exfiltration* : agenti Cyber-raccolta di solito trapelare i dati acquisiti in modo discreto, spesso in attesa per il traffico web di alta e mascherare la trasmissione come la navigazione web sicura. Unità flash USB sono stati utilizzati per trapelare informazioni da spazio d'aria dei sistemi protetti. Sistemi exfiltration spesso comportano l'uso di sistemi proxy inversi Anonimizza il ricevitore dei dati.
- *Replicare* : Gli agenti possono replicarsi su altri supporti o sistemi, ad esempio un agente può infettare i file su una condivisione di rete scrivibile o si installare sul drive USB per infettare i computer protetti da un intercapedine d'aria o comunque non sulla stessa rete.
- *Gestione di file e di manutenzione del file* : Il malware può essere usato per cancellare le tracce di sé dai file di log. Si può anche scaricare e installare i moduli o gli aggiornamenti e file di dati. Questa funzione può anche essere utilizzato per piazzare "prove" sul sistema di destinazione, ad esempio, per inserire la pedopornografia sul computer di un politico o di manipolare voti su una macchina elettronica conteggio dei voti.
- *Regole di combinazione* : Alcuni agenti sono molto complesse e sono in grado di combinare le caratteristiche di cui sopra, al fine di fornire capacità di raccolta di informazioni molto mirate. Ad esempio, l'uso di scatole di delimitazione GPS e l'attività del microfono può essere utilizzato per trasformare uno smartphone in un bug intelligente che intercetta le conversazioni solo all'interno dell'ufficio di un bersaglio.
- *Cellulari compromesse* . Dal momento che, cellulari moderni sono sempre più simili a computer di uso generale, questi cellulari sono vulnerabili agli stessi attacchi informatici-collect come sistemi di computer, e sono vulnerabili a trapelare informazioni estremamente sensibili colloquiale e la posizione per un aggressori. Perdite di posizione cellulare GPS e le informazioni colloquiale per un attaccante è stata riportata in una serie di recenti cyber-inseguendo i casi in cui l'attaccante è stato in grado di utilizzare la posizione GPS della vittima a chiamare le imprese e le autorità di polizia nelle vicinanze per fare false accuse contro la vittima a seconda della sua posizione, questo può variare da dire l'informazione personale del ristorante per prendere in giro la vittima, o fare falsa testimonianza contro la vittima. Per esempio se la vittima fosse parcheggiata nel grande parcheggio gli attaccanti possono chiamare e stato che hanno visto droga o l'attività della violenza in corso con la descrizione della vittima e le indicazioni per la loro posizione GPS.

Infiltrazione

Ci sono diversi modi comuni per infettare o accedere al bersaglio:

- Un *proxy di iniezione* è un sistema che è posto a monte del singolo bersaglio o la società, di solito al provider di servizi Internet, che inietta il malware nel sistema target. Ad esempio, una scarica innocenti da parte dell'utente può essere iniettato con l'eseguibile di malware al volo in modo che il sistema di destinazione è quindi accessibile agli agenti del governo.
- *Spear Phishing* : un e-mail con cura artigianale viene inviato al bersaglio al fine di invogliare loro di installare il malware tramite un Trojan documento o di un'unità da un attacco ospitato su un server web compromesso o controllate dal proprietario del malware.
- *Ingresso fraudolento* può essere utilizzato per infettare un sistema. In altre parole, le spie si rompono con molta prudenza in residenza o la sede del bersaglio e installare il malware sul sistema di destinazione.
- Un *monitor di monte* o *sniffer* è un dispositivo in grado di intercettare e visualizzare i dati trasmessi da un sistema di destinazione. Di solito questo dispositivo è posizionato al provider di servizi Internet. Il Carnivore sistema sviluppato dagli Stati Uniti FBI è un famoso esempio di questo tipo di sistema. Sulla base della stessa logica di un'intercettazione telefonica , questo tipo di sistema è di uso limitato oggi a causa dell'uso diffuso di cifratura durante la trasmissione dei dati.
- Un *infiltrazione wireless* sistema può essere utilizzato in prossimità del bersaglio quando il bersaglio sta utilizzando la tecnologia wireless. Questo è di solito un sistema basato computer portatile che impersona una stazione di WiFi o 3G di base per catturare i sistemi di destinazione e le richieste dei relè a monte a Internet. Una volta che il target sono i sistemi in rete, il sistema funziona quindi come *un'iniezione proxy* o come *monitor a monte* al fine di infiltrarsi o monitorare il sistema di destinazione.
- Una *chiave USB* precaricata con l'untore del malware può essere dato o è sceso al sito di destinazione.

Agenti Cyber-raccolta sono generalmente installati da software di consegna payload costruito utilizzando zero-day attacchi e consegnati tramite unità USB infette, allegati e-mail o siti Web dannosi. Stato sponsorizzato cyber-collezioni sforzi hanno utilizzato certificati ufficiali del sistema operativo al posto di basarsi su vulnerabilità di sicurezza. Nell'operazione Fiamma, Microsoft afferma che il certificato Microsoft ha utilizzato per impersonare un Windows Update è stato forgiato; Tuttavia, alcuni esperti ritengono che potrebbe essere stata acquisita attraverso HUMINT sforzi.