Carnivore (software)

Da Wikipedia, l'enciclopedia libera.

Carnivore (conosciuto anche come **DCS1000** che significa Digital Collection System) è il nome dato ad un sistema, analogo ad un network tap, implementato dall'FBI (Federal Bureau of Investigation), nei suoi laboratori di Quantico (Virginia). Grazie all'utilizzo di questa tecnologia le e-mail vengono controllate così come le conversazioni telefoniche. È una forma di controllo di polizia.

Indice

Storia

Questo sistema è stato messo in funzione dai servizi segreti americani nel periodo immediatamente successivo all'attacco al World Trade Center l'11 settembre 2001 per controllare il traffico in rete e prevenire ulteriori attacchi terroristici.

Con questa piattaforma è possibile intercettare il traffico sui protocolli di navigazione HTTP, FTP, SMTP, e POP3, inviato o diretto a tutte le porte.

L'esistenza di Carnivore viene resa nota il 4 luglio 2000, quando il quotidiano statunitense Wall Street Journal scrive per la prima volta dell'esistenza di Carnivore, nello stesso periodo in cui il senato americano stava dibattendo sul suo possibile impiego.

Soltanto il 26 ottobre 2002 il governo USA concede il via libera per l'utilizzo su larga scala come conseguenza dell'attacco all'America. DCS1000 da allora viene, infatti, inserito all'interno del pacchetto di misure anti-terrorismo chiamato *Patriot Act*[1] per contrastare il terrorismo mondiale ed in particolare l'organizzazione di Al-Qaeda.

Il progetto Carnivore è derivato da una precedente esperienza molto simile denominata "Omnivore", che già permetteva di focalizzare l'attenzione su un particolare utente, controllarlo in ogni suo movimento nel cyberspazio oltre a consentire un'analisi approfondita su tutta la posta elettronica, e dal sistema di sorveglianza "Echelon", messo in atto dalla National Security Agency (NSA) durante il periodo della Guerra Fredda.

Si tratta, quindi, di un programma in grado di filtrare i pacchetti di dati che transitano tra l'utente e il provider e di ricostruire i messaggi scambiati: posta elettronica, pagine web visitate e conversazioni in diretta (chat).

Carnovire può essere definito come uno sniffer, con la differenza che i normali sniffer permettono a chiunque l'accesso come amministratore per controllare il flusso di dati il tipo di indagini che si stanno svolgendo; questo sistema, invece, analizza il traffico della rete solo dopo averlo copiato: in questo modo nessuno può conoscere la quantità e il tipo di informazioni intercettate.

Il Pacchetto Carnivore

- Sistema operativo Windows NT (o Windows 2000);
- 128 MB di RAM Processore Pentium III, disco rigido da 4-18 GB di spazio in disco e un drive lomega Jaz da 2 Gb sul quale vengono salvati i dati;
- La macchina non ha uscite TCP/IP per evitare intrusioni da parte degli Hacker;
- Sistema hardware di autenticazione per controllare gli accessi alla macchina impedendo accessi non autorizzati;
- Software scritto in C++ (si distinguono tre diversi programmi: Carnivore, Packeteer, Coolminer).

Il sistema

Il sistema si compone di un computer collegato presso un provider, che copia tutti i dati: esso si inserisce nel segmento della rete in cui si trova la persona sospetta, non interagisce, né intralcia il flusso comunicativo, limitandosi esclusivamente a copiarlo.

I pacchetti di dati così copiati con il software Carnivore vengono automaticamente analizzati da un filtro che cerca le parole o i termini considerati motivo di sospetto dalla polizia federale americana; tutto il materiale ininfluente viene, al contrario, eliminato, anche per occupare il minor spazio possibile in memoria.

I dati vengono trasmessi tramite linea telefonica al client "Packeteer" che ricostruisce i file sulla base delle intercettazioni, il risultato viene successivamente inviato agli operatori federali con l'aiuto del terzo software del pacchetto chiamato "Coolminer", salvato e copiato su un particolare tipo di disco Jaz che quotidianamente viene scaricato dagli uomini dell'FBI.

Le operazioni di copiatura dei dati non rallentano il flusso comunicativo, per cui la presenza di Carnivore nel server è impercettibile; non si tratta di un sistema molto veloce, ma in grado comunque di elaborare milioni di e-mail al secondo.

Il costo del pacchetto è stimato intorno ad un milione di euro.

La procedura per l'installazione del DCS1000 è molto semplice: una volta individuato il soggetto sospetto da controllare, l'FBI chiede al giudice l'autorizzazione per le intercettazioni, specificando che le informazioni rientrano nell'ambito di un'inchiesta penale.

Ottenuto il permesso viene ricercato il provider interessato e si installa il pacchetto che è molto simile alla scatola nera degli aerei, perfettamente sigillata. Periodicamente i poliziotti scaricano e verificano i dati raccolti.

Il governo statunitense potrà confermare o negare il funzionamento del sistema, ma ci sono alcuni aspetti che generalmente sono accettati. Un computer per essere accessibile deve essere fisicamente installato in un ISP o in un'altra locazione dove si può "sniffare" il traffico per cercare messaggi email in transito. La tecnologia non richiede niente di particolare, basta usare un comune packet sniffer o qualcosa di simile (come uno script perl ad esempio).

Si può ottenere la cooperazione degli ISP o dei gestori di una LAN dove installare Carnivore sia volontariamente sia su mandato; una volta che il sistema è piazzato non è solo abilitato a catturare semplicemente ogni email che attraversa il sistema, ma può anche inviare un avvertimento nominando specifiche persone o email che possono essere monitorate. Quando una email equivale a questi criteri, il messaggio viene annotato con le informazioni desiderate come la data, l'ora, il destinatario e il mittente. Tale intercettazione può anche essere inviato immediatamente all'FBI, ma attualmente non si conoscono i dettagli.

Dal momento in cui è stata resa nota l'esistenza di questo sistema, sono nate controverse polemiche legate alle possibili violazione della privacy che questo nuovo strumento di sorveglianza poteva facilmente attaccare: i difensori della sfera privata hanno iniziato una mobilitazione per frenare la curiosità di Carnivore

In particolare tra le misure preventive per tutelare la libertà personale rientra la creazione di programmi anti-Carnivore come il software criptografico chiamato "Antivore" lanciato dalla software House ChainMail; oppure "Camera Sky" in grado di nascondere i dati eludendoli al controllo del DCS1000, infine altri due software come "Freedom" ideato da "Zeroknowledge" e quello della società "NetworIce".

L'FBI ha sempre sostenuto che il DCS100 non avrebbe pregiudicato la privacy dei navigatori poiché, grazie a filtri speciali (che possono essere modificati all'insaputa del provider), esso è in grado di intercettare solo le informazioni sensibili, una rassicurazione non priva di polemiche.

Inoltre, il già citato, "Patriot Act" fornisce alla polizia informatica americana la libertà di perseguire Hacker stranieri accusati di avere commesso crimini sulla rete degli USA.

La polizia federale ha ammesso di avere usato Carnivore in venticinque casi di cui sedici nel 2000 d cui sei criminali e dieci di spionaggio e terrorismo.

Ci sono diverse speculazioni riguardo l'implementazione, l'uso, e i possibili abusi di Carnivore. Ma i fautori di Free speech e dei diritti civili sono interessati sul potenziale di questo strumento.

L'assistente del direttore dell'FBI Director Donald Kerr ha affermato:

> *Il sistema Carnivore funziona più o meno come uno "sniffer" e altri strumenti di diagnostica delle reti usati dagli ISP quotidianamente, tranne che fornisce all'FBI l'unica abilità di distinguere tra comunicazioni che potrebbero essere o non essere legittimamente intercettate. Per esempio, se un mandato prevede l'intercettazione legale di un tipo di comunicazione (per esempio, e-mail), ma esclude gli altri (per esempio, online shopping) lo strumento può essere configurato a intercettare solo e-mail che vengono trasmesse da e per un certo nome. È un analizzatore di reti molto specializzato che funziona come un applicativo su un normale PC sotto il sistema operativo Microsoft Windows. Funziona come "sniffing" di una determinata porzione di rete e copiando e memorizzando solo i pacchetti che uguagliano precisamente un definito filtro configurato in conformità al mandato. Questo filtro può essere molto complesso e fornisce all'FBI la capacità di raggruppare trasmissioni che si conformano ai mandati scritti, ai mandati "trap & trace", agli ordini di intercettazione Titolo III, ecc. È importante distinguere ora cosa significa "sniffing." Il problema di discernere tra i messaggi degli utenti di Internet è complesso. Tuttavia ciò che esattamente Carnivore fa è che non cerca nel contenuto di ogni messaggio collezionando quelli che contengono una certa parola come "bomba" o "droga", ma seleziona i messaggi basati su criteri espressi nel mandato, per esempio, messaggi trasmessi da e per un particolare account o utente. cryptome.org (http://cryptome.org/carnivore-rf.htm)*

L'FBI non si è però fermata a Carnivore iniziando ad utilizzare nuovi sistemi tra i quali: Dragon Ware utile per tracciare ogni movimento del sospetto in rete e "Magic Lantern". Quest'ultimo funzione come un "Trojan Horse" (letteralmente "Cavallo di Troia"), un programma che si installa sul computer del soggetto da controllare e compie una serie di attività tra le quali quella di registrare i tasti premuti sulla tastiera in modo da captare parole sospette (come attentati, terrorismo, ecc.) oltre a fornire chiavi di accesso, password e modalità di decifrazione dei documenti criptati. Il meccanismo che permette di rilevare la chiave di accesso in gergo è chiamato "Keylogging", cioè memorizza le parole inserite dalla tastiera in un file particolare che, una volta elaborato, permette di risalire alla parola chiave. In questo modo, potendo vedere i tasti è possibile risalire a password, testi scritti, programmi eseguiti, indirizzi internet visitati.

La polizia federale americana non ha mai voluto rendere pubblico il codice sorgente di questo sistema per tre ragioni:

- Perché gli hacker potrebbero violare il sistema;
- Perché esso è protetto da copyright e quindi non è possibile diffonderlo per esigenze contrattuali;
- La legislazione degli Stati Uniti (Titolo 18 Sezione 2512 del Codice) impedisce la diffusione di apparecchiature studiate per spiare clandestinamente le comunicazioni di altre persone.

Nonostante questo, la legge americana sulla libertà di informazione ha consentito all'EPIC (Electronic Privacy Information Center) di ottenere 565 pagine di documenti riservati su Carnivore, alcune delle quali sono però state in parte mascherate con inchiostro indelebile tra cui proprio quelle del codice sorgente.

Dopo i prolungati attacchi della stampa, l'FBI ha cambiato il nome di questo sistema da "Carnivore" a "DCS1000."

A metà gennaio 2005 l'FBI essenzialmente abbandona Carnivore in favore di software commerciali[2]. Le motivazioni che hanno spinto la polizia federale verso questa scelta riguardano le forti critiche dell'opinione pubblica contro questo sistema più volte accusato di violare la libertà personale dei cittadini.

Altre applicazioni pratiche

> **Questa voce o sezione sull'argomento internet non cita le fonti necessarie o quelle presenti sono insufficienti**.

Esiste, infine, un'altra faccia di Carnivore. Un gruppo di net-artisti interessati alla sperimentazione digitale i "Radical Software Group" (RSG) di New York, hanno clonato il software creato dalla polizia federale americana, per utilizzarlo con degli scopi diversi. Si tratta di una piattaforma situata nella loro città per la net-art chiamata "CarnivorePE", che ha lo scopo di catturare i pacchetti di dati e trasformarli successivamente in musica, immagini o filmati; in questo modo i dati diventano arte.

Il programma è stato messo a disposizione dal RSG di una vasta comunità di altri artisti. Tra questi, un gruppo di italiani chiamato "Limiteazero" ha visto in Carnivore una nuova forma di ready made. Essi hanno sperimentato due forme di arte con questo sniffer: una sperimentazione software chiamata *"Actiwe Metaphore"* (2002) e una hardware denominata *"Network is Speaking"* (2004).

La prima traduce gli indirizzi e i dati intercettati in forme tridimensionali, movimenti e suoni, in questo modo il flusso dei dati, normalmente percepibile solo dalla macchina, viene reso visibile a tutti. La seconda, invece, è un'installazione molto complessa allestita a Milano, essa ricorda la forma di Idra dove le dodici teste del mostro sono rappresentate da 12 monitor LCD appesi al soffitto.

Infine, altri due esempi di arte emergente riguardano: "Policestate" che converte i dati catturati in movimenti per modellini delle macchinine radio comandate dalla polizia, con movimenti a volte disordinati e altre organizzati in modo da formare vere e proprie coreografie; "Word Wide Painters" che trasforma i dati ricevuti in graffiti sul muro, talvolta riproducendo le bandiere dei paesi di provenienza dei soggetti spiati, i loro indirizzi IP o i siti a cui si connettono, naturalmente in assoluto rispetto della privacy degli utenti.

Note

1. **^** Le mani dell'FBI su Internet | Diritto online | Webnews (http://webnews.html.it/news/leggi/3594/le-mani-dellfbi-su-internet/) Archiviato (https://web.archive.org/web/20060607215552/http://webnews.html.it/news/leggi/3594/le-mani-dellfbi-su-internet/) il 7 giugno 2006 in Internet Archive.
2. **^** *FOXNews.com - FBI Ditches Carnivore Surveillance System - Politics*, su *foxnews.com*. URL consultato il 15 febbraio 2005 (archiviato dall'url originale il 22 agosto 2006).

Voci correlate

- Digital Collection System Network

- Sniffing, intercettazione passiva dei dati nella rete
- Magic Lantern software, lo strumento di login simultanea dell'FBI
- Regulation of Investigatory Powers Act, provvedimento legale inglese per l'intercettazione digitale
- ECHELON, programma di intercettazione digitale mondiale
- DragonWare Suite, programma FBI per immagazzinare le informazioni di siti web
- Total Information Awareness
- Patriot-Act, insieme di misure anti-terrorismo adottate negli USA dopo l'11 settembre 2001

Collegamenti esterni

- (EN) *Cryptome on Carnivore*, su *cryptome.org*.
- (EN) *Wired on Carnivore*, su *wired.com*.
- (EN) *EPIC on Carnivore*, su *epic.org*.
