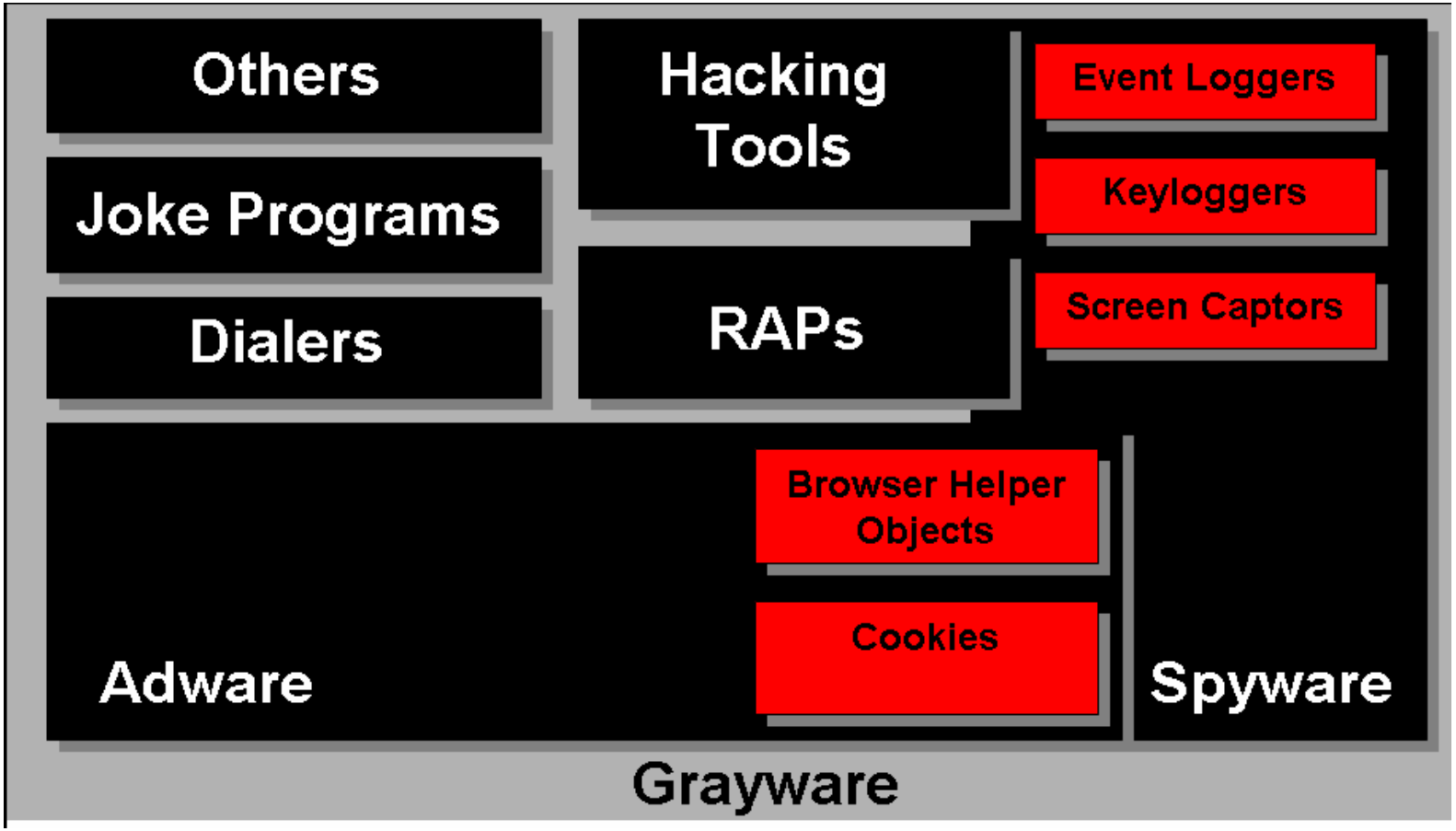
Spyware,come fronteggiare una delle minacce più diffuse

Patrick Gada
Senior Sales Engineer

18 ottobre 2005

TREND MICRO

Grayware



TREND MICRO

Spyware

E’ un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata. Programmi per la raccolta di dati che vengano installati con il consenso dell'utente non sono propriamente spyware, sempre che sia ben chiaro all'utente quali dati siano oggetto della raccolta e a quali condizioni questa avvenga (purtroppo avviene molto raramente).

Categorie di Spyware

- *Browser Helper Objects (Browser Hijackers)*
- *Finestre pubblicitarie di pop-up (Adware)*
- *Winsock Hijackers*
- *Man-in-the-middle Proxies*
- *Ad-serving o Tracking Cookies*
- *Ransomware*
- *Keyloggers (Keystroke Monitoring)*
- *Dialers*

TREND MICRO

Browser Helper Objects (Browser Hijackers)

Browser "Hijacker" ("dirottatore")

Sono applicazioni (librerie di programma) che si installano come plug-in di IE o altro browser aggiungendo nuove barre degli strumenti, barre di ricerca ecc..)

Sono in grado di modificare qualsiasi tipo di impostazioni del browser (es. pagina di default iniziale, la pagina di errore o di ricerca, l'elenco dei preferiti, ecc…), dirottare le richieste web, mostrare finestre di pop-up pubblicitarie e inviare informazioni all'esterno.

Browser Helper Objects (Browser Hijackers)

***CoolWebSearch** è il nome dato a una vasta varietà di differenti browser hijackers.*

Gli utenti che inseriscono un indirizzo sbagliato vengono dirottati verso un sito chiamato coolwebsearch.com (o altri siti affiliati).

Trend Micro CWShredder e AntiSpyware (servizi on-line)

http://www.trendmicro.com/cwshredder

http://www.trendmicro.com/spyware-scan/

TREND MICRO

Browser Helper Objects (Browser Hijackers)

Esempio:

XXXToolbar

Tipo: Browser Helper Object

Descrizione ufficiale: programma che crea messaggi pubblicitari sul proprio PC.

URL: http://www.xxxtoolbar.com

Proprietà:

- *usa tattiche di tipo stealth*
- *rimane residente*
- *mostra messaggi pubblicitari*
- *cambia la configurazione del browser*

TREND MICRO

Adware

Visualizzano banner pubblicitari sul computer dell'utente, registrano le abitudini di navigazione e le trasmettono ad un server che svolge la funzione di centrale di smistamento per l'invio di messaggi pubblicitari mirati.

Le finestre di pop-up pubblicitarie non sono casuali ma si basano sulle abitudini di navigazione dell'utente.

Es. Cydoor e Gator sono classificati come Adware

La versione free di Kazaa incorpora GAIN (Gator), Cydoor e la barra di ricerca MyWay

Winsock Hijacker

Sono applicazioni Spyware che installano un LSP (Layered Service Provider) che situato fra gli strati "Winsock" del S.O. si "agganciano" al protocollo TCP/IP per monitore le connessioni di rete (visi visitati, frequenza, ecc…)

Di default sul S.O. Windows sono installati numerosi LSP utili.

Sono difficili da rimuovere in quanto si può interrompere la catena a livello LSP e quindi l'accesso a Internet.

Alcune varianti di CoolWebSearch sono Winsock Hijcker.

Man in the middle Proxies

Con la promessa di accelerare la connessione ad Internet, questo Spyware dirotta tutte le richieste web comprese le connessioni sicure, verso un proxy “man in the middle”.

Es. Marketscore

From the privacy agreement 02.07.05:

"Marketscore monitors all of your Internet behavior, including both the normal web browsing you perform, and also the activity you may have through secure sessions, such as when filling a shopping basket or filling out an application form that may contain personal financial and health information. Marketscore's proprietary and patent pending technology allows us to see the details of secure pages while protecting such content from parties other than the site to which you are connected."

"In addition to the monitoring of your Internet behavior, we may also combine the information that you provide us with information such as credit or prescription information that we obtain from third parties such as consumer preference reporting companies, credit reporting agencies, and prescription benefits managers."

Ad-serving o Tracking Cookies

I Cooky vengono generalmente utilizzati dalle applicazioni web per mantenere lo stato sulle sessioni e sono quindi utili ad es. per le applicazioni di commercio elettronico per tenere traccia degli articoli acquistati (carrello della spesa).

Al contrario i "tracking Cookies" tracciano le abitudini web attraverso la navigazione degli utenti su siti fra loro non correlati e differenti per tipologia ma legati alla stessa rete pubbicitaria.

Es di aziende che usano i tracking cookies:

Doubleclick, LinkShare, Commission Junction, ecc..

Ad-serving o Tracking Cookies

Le informazioni che vengono raccolte comprendono:

- *Indirizzo IP*
- *Tipo di browser*
- *Sistema operativo*
- *Nome del dominio*
- *Service Provider*
- *Local time zone*

TREND MICRO

“Ransomware”

Sono programmi che cifrano i file sulle macchine degli utenti che ne sono vittime.

Viene solitamente utilizzato un programma trojan che ad un certo punto inizia a cifrare i file e successivamente viene richiesto un riscatto per poter ottenere la chiave di decifrazione.

Ad es. SpywareAssasin, SpywareNo.

TROJ_PGPCODER varianti A e B

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PGPCODER.A

TROJ_PGPCODER.A

This memory-resident Trojan arrives via Internet or copied from disks. Upon execution, it encrypts all files on the system having the following extensions:

ASC
DB
DB1
DB2
DBF
DOC
HTM
HTML
JPG
PGP
RAR
RTF
TXT
XLS
ZIP

As a consequence, the files with the above-mentioned extensions become unreadable after infection.

Keylogger (Keystroke Monitoring)

Memorizza la sequenza di tasti premuti sulla tastiera per carpire informazioni personali quali password, numero di carta di credito, ecc..

Esistono due tipi di categorie:

- *keylogger commerciali*
- *Keylogger “custom.built” installati a seguito di un attacco.*

Dialer

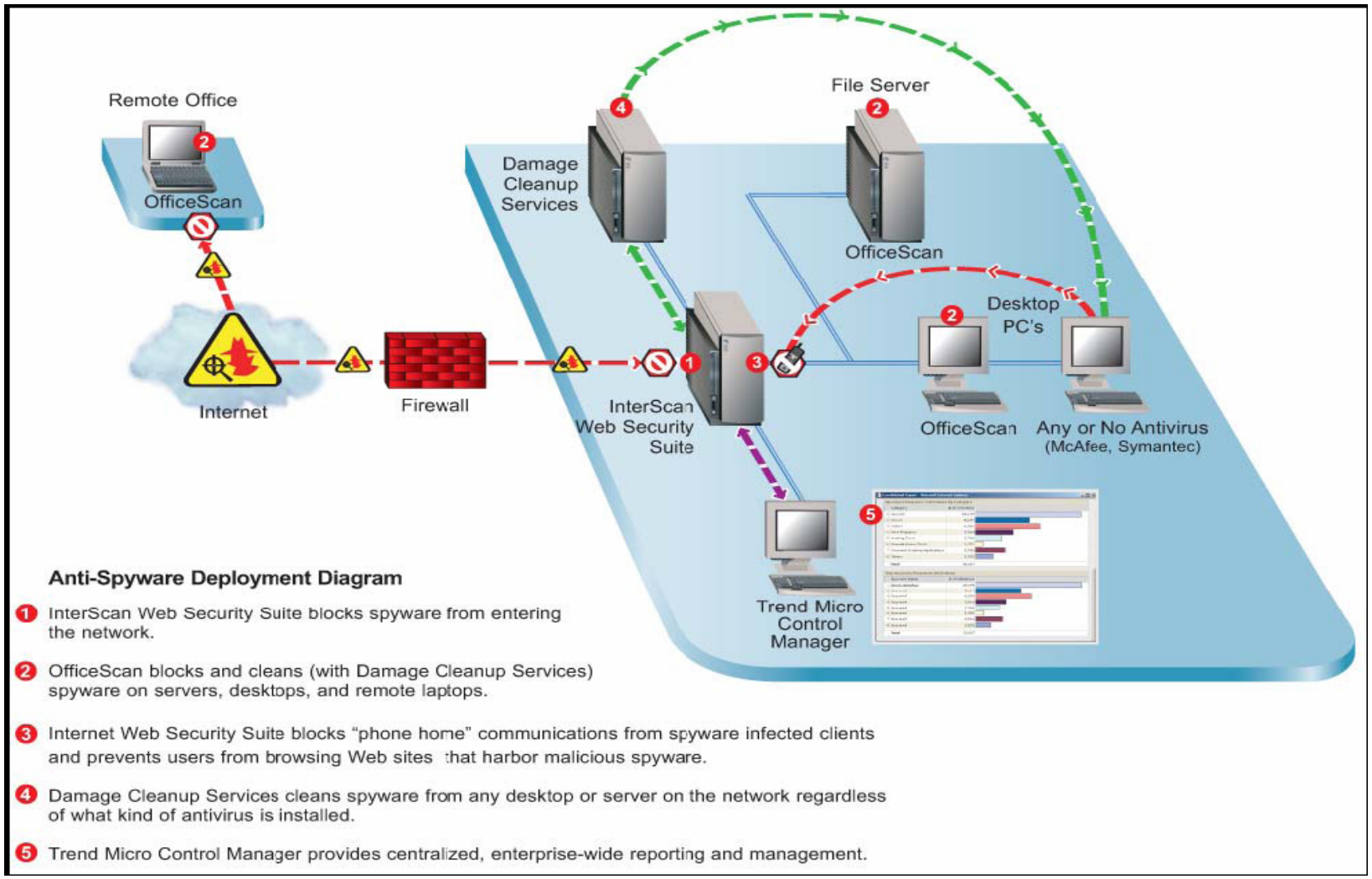
Modificano la normale connessione al provider Internet allo scopo di aumentare la tariffa telefonica dell'utente con chiamate ad es. verso numeri a pagamento ad alto costo, numeri internazionali, satellitari, ecc...

Metodi di infezione

- *Download o script automatici (Drive-by Downloads)*
- *Installazione incorporata in applicazioni gratuite*
- *Incorporate in applicazioni di tipo file-sharing P2P*
- *Ingegneria sociale*
- *Sfruttando vulnerabilità a livello applicativo (es. IE o exploit JPEG)*

TREND MICRO

Come prevenire?



TREND MICRO

Phishing

Tecnica di attacco di ingegneria sociale utilizzata per carpire informazioni personali e riservate (numero di conto corrente, numero di carta di credito, pawwsord, ecc..) mediante l'utilizzo di messaggi di posta elettronica fasulli opportunamente creati per apparire autentici.

Pharming

L'obiettivo è sempre quello di carpire informazioni personali e riservate (numero di conto corrente, numero di carta di credito, pawwsord, ecc..)

Tecnica di attacco che sfrutta le vulnerabilità del server DNS con l'obiettivo di alterare l'indirizzo IP di un sito web con quello di un sito trappola.