VIRUS: FIZZER

"fizzer è capace di catturare tutto quello che la sua vittima digita e di conservarlo in un file che può essere successivamente scaricato da un intruso, ottenendo così dati che possono compromettere la sicurezza e la privacy dell'utente infettato."

1. COS'È?

Fizzer è un worm pericoloso, è stato infatti progettato per registrare tutto quanto venga digitato nella tastiera dell'utente del computer colpito e conservarlo in un file di testo.
In questo modo, qualsiasi hacker che acceda a questo file può ottenere informazioni riservate dell'utente, come password d'accesso a certi servizi, programmi chat, posta elettronica, chiavi di accesso a conti bancari, eccetera.
Inoltre, Fizzer è stato predisposto per eliminare definitivamente certi processi legati ai programmi antivirus.
Fizzer si propaga principalmente attraverso i programmi di chat IRC e la posta elettronica. Invia una copia di sé stesso a tutti i contatti che trova nella Rubrica di Windows.

2. QUANTI TIPI VE NE SONO?

Alias:W32/Fizzer@MM (McAfee), W32/Fizzer-A (Sophos), W32/Fizzer (Panda Software), WORM_FIZZER.A (Trend Micro), W32.HLLW.Fizzer@mm (Symantec), Win32.Fizzer.A@mm (Bit Defender), W32/Fizzer (Hacksoft), Fizzer (F-Secure), I-Worm.Fizzer (Kaspersky (viruslist.com)), Win32.Fizzer (Computer Associates), Win32/Fizzer.A@mm (RAV)

3. COME AGISCE?

Le distinte componenti del worm si incaricano dei seguenti compiti:
1. Catturare gli indirizzi della Rubrica di Outlook
2. Catturare gli indirizzi della Rubrica di Windows (WAB)
3. Catturare gli indirizzi trovati nel sistema locale
4. Generare in maniera aleatoria indirizzi
5. Lanciare IRC bot, Internet Relay Chat,
6. Lanciare AIM bot (AOL Instant Messenger)
7. Keylogger
8. Worm da propagare attraverso KaZaa
9. Server HTTP

10. Terminare il software Anti-virus.
11. Il worm contiene il suo proprio motore SMTP, ma può anche usare quello stabilito nella configurazione del registro del sistema.
12. Arriverà in un file allegato ad alcuno dei vari tipi di messaggi che utilizza per la sua propagazione. Il contenuto del campo From (da) può perfettamente non essere quello dell'emittente originale. Il corpo del messaggio ed il tema possono avere contenuti diversi. Le estensioni dei file allegati potranno essere . com, .exe. pif. scr.

I **messaggi** saranno del tipo:
Subject: why?
Body: The peace
Attachment: desktop.scr

Subject: Re: You might not appreciate this...
Body: lautlach
Attachment: service.scr

Subject: Re: how are you?
Body: I sent this program (Sparky) from anonymous places on the net
Attachment: Jesse20.exe

Subject: Fwd: Mariss995
Body: There is only one good, knowledge, and one evil, ignorance.
Attachment: Mariss995.exe

Subject: Re: The way I feel - Remy Shand
Body: Nein
Attachment: Jordan6.pif
Quando viene eseguito l'allegato realizzerà le seguenti **task**:
1. Estrarrà vari file copiandoli sulla directory (%WinDir%).
    a. initbak.dat (220,160 byte) - Copia del worm
    b. iservc.exe (220,160 byte) - Copia del worm
    c. ProgOp.exe (15,360 byte) – Dropper
    d. iservc.dll (7,680 byte) - Controller temporaneo.

2. Creerà questa chiave nel registro per essere attivato quando si avvia Windows:
    HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
    Run "SystemInit" = C:\WINDOWS\ISERVC.EXE

3. Modificherà il registro per permettere al worm di attivarsi ogni volta che si apra un file del tipo TXT:
    HKEY_CLASSES_ROOT\txtfile\shell\open\command
    (Predeterminado) =
    c:\windows\PROGOP.EXE 0 7 ' c:\windows\NOTEPAD.EXE %1'
    'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'

4. Ripeterà l'azione precedente per il seguente registro:
    HKCR\Applications\ProgOp.exe\shell\Open\Command
    (Predeterminado) =
    c:\windows\PROGOP.EXE 0 7 ' c:\windows\NOTEPAD.EXE %1'
    'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'

5. Nel sistema WinNT/2K/XP genererà un processo denominato S1TRACE.

Nota: In tutti i casi" C:\Windows" può variare in funzione del sistema operativo installato (con questo nome per difetto in Windows 9x/ME e XP e come" C:\WinNT" in Windows NT/2000).

Routine di invio massivo
Utilizzerà il suo proprio motore SMTP per spedirsi a tutte gli indirizzi della rubrica di Outlook ed a indirizzi generati in modo aleatorio come:

- Nomi aleatori raccolti da una lista interna del worm
- Numeri aleatori
- Nomi di domino aleatori (@ dominio) raccolti dalla seguente lista interna:
    - aol.com
    - earthlink.com
    - gte.net
    - hotmail.com
    - juno.com
    - msn.com
    - netzero.com
    - yahoo.com

Tema, messaggio e nome del file allegato vengono generati usando in modo aleatorio diverse catene di testo come:
"So how are you?"
"Check it out"
"There is only one good, knowledge, and on evil, ignorance"
"I sent this program (sparky) from anonymous places on the net"
"you must not show this to anyone"
"Today is a good day to die"
"thought I'd let you know"
"The way to gain a good reputation is to endeavor to be what you desire ..."
"Filth is a death"
"wie geht es Ihnen?"
"Philosophy imputes, reinterprets faith"
"If you don't like it, just delete it"
"delete this as soon as you lokk at it"
"Did you ever stop to think that viruses are good for the economy? ..."
"the incredibly bright faith"
"you don't have to if you don't want to"
"I wonder what can be so bad ..."

"Watchin' the game, having a bud."
"the attachment is only for you to look at"
"Let me know what you think of this..."

IRC Bot:

Invia anche copie agli utenti connessi ai canali di chat visitati dalla vittima.
Inoltre, invia PING a differenti server IRC, generalmente attraverso la porta TCP/6667. PING (Packet Internet Groper) è un comando usato per comprovare le connessioni ad uno o più host remoti inviando un pacchetto di byte che normalmente viene restituito come eco.

Quando riceve una risposta, si connette ad un canale usando differenti nomi di una lista interna e rimane in attesa delle istruzioni di un attaccante, agendo come un BOT (copia di un utente in un canale di IRC, preparata a rispondere a determinati comandi che le vengono inviati a distanza, in modo da riuscire a svolgere molteplici azioni coordinate simultaneamente).

Questa è la lista di server IRC:

1. irc2p2pchat.net
2. irc.idigital-web.com
3. irc.cyberchat.org
4. irc.othernet.org
5. irc.beyondirc.net
6. irc.chatx.net
7. irc.cyberarmy.com
8. irc.gameslink.net

Propagazione attraverso KaZaA:

Per diffondersi attraverso questo programma di filesharing punto a punto, opera seguendo questi i passi:
. Crea all'interno della directory condivisa varie copie di se stesso. Queste copie avranno nomi aleatori.
. Altri utenti di KaZaA possono accedere a questa directory condivisa. In questo modo, scaricheranno volontariamente nei loro computer alcuni di questi file, credendo che si tratti di applicazioni interessanti. In realtà, staranno scaricando nei loro computer una copia del worm.
. Quando questi utenti eseguono il file scaricato, rimangono infettati.

Keylogger: Intercettatore delle battute della tastiera.

Registrano le battute della tastiera realizzate dall'utente. Fizzer conserva le battute in un file di testo da lui stesso creato nella directory di Windows, chiamato ISERVC.KLG. Successivamente lo cripta. Se un hacker entra in possesso di questo file, avrà un accesso completo a dati confidenziali dell'utente del computer colpito, come chiavi di accesso a servizi Internet, conti bancari, etc.

Terminazione del software Anti-virus

Per evitare di essere scoperto, termina i processi le cui denominazioni contengano le seguenti catene:

- ANTIV
- AVP
- F-PROT
- NMAIN
- SCAN
- TASKM
- VIRUS
- VSHW
- VSS

4. COME ELIMINARLO?

Antivirus

1. Mantenga sempre aggiornato il suo anti-virus con le ultime definizioni
2. Esegua la scansione completa analizzando tutti i suoi dischi
3. Cancelli i file che si rivelino infettati

Cancellazione manuale dei file creati dal virus

Dall'Esploratore di Windows, localizzi e cancelli i seguenti file:
c:\windows\ISERVC.KLG
c:\windows\INITBAK.DAT
c:\windows\ISERVC.EXE
c:\windows\ISERVC.DLL
c:\windows\PROGOP.EXE

Clicchi con il tasto destro sull'icona del " Cestino" nel Desktop e selezioni "Svuota cestino".
Cancelli anche i messaggi elettronici del tipo di quelli precedentemente indicati.

Modificare il registro

1.Apra l'Editor del registro: "Avvio" , "Esegui", scriva "REGEDIT" e prema ENTER
2.Nel pannello sinistro dell'Editor, clicchi sul simbolo "+" fino ad espandere la seguente chiave:
HKEY_LOCAL_MACHINE
\SOFTWARE
\Microsoft
\Windows
\CurrentVersion
\Run

3. Clicchi sulla cartella "Run" e nel riquadro a destra, sotto la colonna" Nomi", cerchi e cancelli il seguente valore:
SystemInit

4. Nel riquadro sinistro del Editor, clicchi sul simbolo "+" fino ad espandere la seguente chiave:
HKEY_CLASSES_ROOT
\txtfile
\shell
\open
\command

5. Clicchi nella cartella "command" e nel riquadro a destra, sotto la colonna "Nome", modifichi poi il contenuto di (Predeterminato) sostituendolo con questi valori:
(Predeterminado) = C:\WINDOWS\NOTEPAD.EXE %1

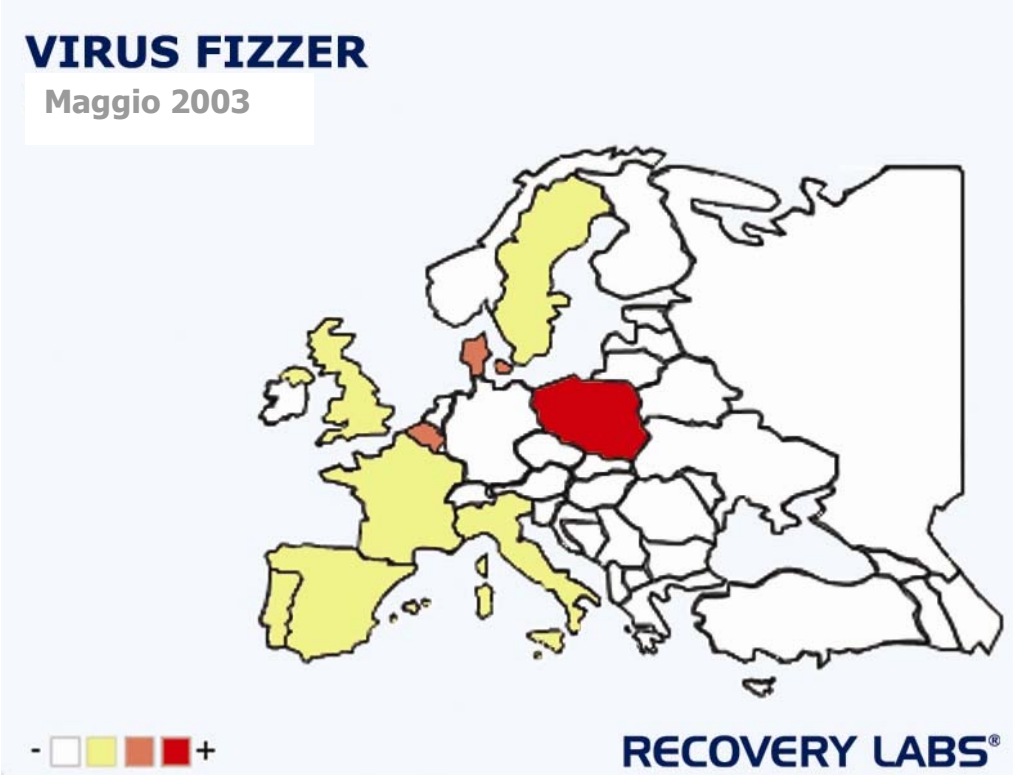
6. Nel riquadro sinistro di Editor, clicchi sul simbolo "+" fino ad espandere la seguente chiave:
HKEY_CLASSES_ROOT
\Applications
\ProgOp.exe

7. Clicchi sulla cartella "ProgOp.exe" e la cancelli.

8. Usi "Registro", "Esci" para salir del Editor e salvare le modificazioni.

9. Riavvii il computer (Avvio, Spegni Computer, Riavvia).

Nota: In tutti i casi" C:\Windows" può variare in funzione del sistema operativo installato (con questo nome per difetto in Windows 9x/ME e XP, e come" C:\WinNT" in Windows NT/2000).


VIRUS FIZZER
Maggio 2003
-
+
RECOVERY LABS®