VIRUS: OPASERV

"La sua capacità di propagazione attraverso le reti lo rende un codice malizioso di fortissimo potenziale infettivo per l'utenza aziendale."

1. COS'È?

Famiglia di worm W32/OPASERV, W32/OPASOFT, I.worm.Opaserv
Dal mese di Settembre del 2002 fino ad oggi, una famiglia di worm ha costituito una continua minaccia in Internet ed ha causato confusione tra alcuni sviluppatori di antivirus, che gli hanno assegnato un nome unico, con differenti estensioni. Attualmente si è arrivati alla versione M o N.
È importante rilevare che un virus possiede una struttura di programmazione definita e se suo autore genera delle varianti, queste presentano solamente leggere modificazioni del payload o semplicemente cambiamenti nel nome o nell'estensione del file infettore.
In caso contrario, ci si troverebbe di fronte ad un nuovo virus o, più specificamente, un nuovo worm.
Questa famiglia è completamente sotto contro, è infatti sufficiente eseguire una routine Euristica specifica per la sua struttura virale che è già ben nota. Indicheremo quindi le sue varianti più significative, senza estenderci in tecnicismi irrilevanti per la maggior parte degli utenti.

2. QUANTI TIPI VE NE SONO?

OPASERV.E è una variante che quando viene eseguita è capace di decriptare il suo codice e di auto-copiarsi su %Windows% come **BRASIL.PIF** o **BRASIL.EXE**.
Crea le seguenti chiavi di registro per essere eseguito ad ogni avvio del sistema:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
Brasil=%Windows%\BRASIL.PIF
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
Brasil=%Windows%\BRASIL.EXE

Il worm propaga i file infettati BRASIL.PIF o BRASIL.EXE e li esegue come un processo che non viene mostrato nella Barra Task di Windows.
Infetta attraverso le unità che condividono C :\ e cerca i computer che abbiano completo accesso alla rete, servendosi della vulnerabilità dello Share Level Password di Windows (Livello condiviso di Password), che consente ad un intruso, in modo remoto, di accedere ai sistemi senza bisogno di conoscere le Password d'accesso.
La security patch per questa vulnerabilità può essere scaricata da:
http://www.microsoft.com/technet/security/bulletin/ms00-072.asp

OPASERV.G è stato rilevato nell'Ottobre 2002, membro della stessa famiglia e variante del worm **Opasoft**, che è stato segnalato nel Settembre 2002, entrambi sono stati creati dallo stesso autore che, a partire dalla prima versione, ha sviluppato e propagato successive varianti, con differenti nomi di file con estensioni **.EXE**, **PIF**, **SCR**, etc., che comunque mantengono la stessa struttura virale.
Quest'ultima occupa 28 KB ed è capace di sviluppare una routine d'accesso abusivo, o **backdoor** che si propaga attraverso reti locali e condivise, utilizzando i servizi di **NETBIOS** di MS Windows.
È un **PE** (Portabile Eseguibile) ed infetta tutti i sistemi operativi.
Windows95/98/NT/Me/2000/XP, compresi server **NT/2000.**
Il worm si auto-installa nella directory di Windows come: **scrsvr.exe** e lo aggiunge alla chiave di registro per essere eseguito nel successivo avvio del sistema:

[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
ScrSvr ="% nome_del_worm%"
Questo worm scansiona i sub-net attraverso la **porta 137** di Servizio del NETBIOS e cerca determinati indirizzi IP all'interno delle unità di reti, se rileva che uno o più computer mantengono aperto il servizio" File and Print Sharing", comincia il suo processo di infezione, assumendone il controllo in modo remoto.

OPASERV.F si propaga attraverso i computer che condividono l'unità C :\ con accesso completo alla rete nella quale si è generata l'infezione, e per realizzare il suo obiettivo si serve del comando **SMB** (Server Message Block Protocol) per accedere alle unità condivise.
Questo worm invia informazioni ad un sito web, attualmente disattivato, dal quale scarica i file infettati **mane!!.dat** e **FDP!!!!.dat** e li installa nella directory radice C :\ , gli stessi file che sono usati per lo scambio di informazioni con il portale ubicato in Brasile.
Nei computer remoti il worm crea il file GAY.INI in C :\ e lo sovrascrive su: % Windows%\win.ini e crea questa chiave di registro per poter essere eseguito nel successivo avvio del sistema:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
cronos ="% Windows%\MARCO!. SCR"
%Windows%, è una variabile che per difetto è "C:\Windows" in Windows 95/98/Me/XP e "C:\Winnt" nel NT/2000.

OPASERV.H si propaga attraverso i computer che condividono l'unità C :\ e si auto-copia alla directory: % Windows% come **MSTASK.EXE**, lo sovrascrive anche su: % Windows%\win.ini e crea questa chiave di registro per essere eseguito nel successivo avvio del sistema:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask ="% Windows%\MSTASK.EXE"

OPASERV.I si propaga attraverso i computer che condividono l'unità C :\ e si auto-copia alla directory: % Windows% come MQBKUP.EXE, lo sovrascrive anche su: % Windows%\win.ini e crea questa chiave di registro per essere eseguito nel successivo avvio del sistema:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mqbkup ="% Windows%\MQBKUP.EXE"
Il worm si attiva il 24 Dicembre 2002 o in date posteriori e mostra un messaggio all'interno di una finestra MS-DOS per poi cancellare il contenuto della CMOS e dell' hard disk:

> NOTICE:
> Illegal Microsoft Windows license detected!
> You are in violation of the Digital Millennium Copyright Act
> Your unauthorized license has been revoked
> For more information, please call us at:
> NOPIRACY
> If you are outside the USA, please look up the correct contact information on our website, at:
> www.bsa.org
> Business Software Alliance
> Promoting a safe & legal online world

OPASERV.J (alcuni anti-virus lo denominano Opaserv L/M/N), rilevato il 27 Dicembre 2002, si propaga nelle unità che condividono l'unità C :\ e si auto-copia nella directory: "% Windows%" come MSTASK.EXE, lo sovrascrive anche su: % Windows%\win.ini e crea questa chiave di registro per essere eseguito nel successivo avvio del sistema:
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask ="% Windows%\MSTASK.EXE"
Infetta attraverso le unità che condividono C :\ e cerca i computer che abbiano completo accesso alla rete, servendosi della vulnerabilità dello **Share Level Password** di Windows
La security patch per questa vulnerabilità può essere scaricata da:
http://www.microsoft.com/technet/security/bulletin/ms00-072.asp

Mostra lo stesso messaggio che abbiamo già visto nel caso dell'**Opaserv.I** e riavvia il sistema.

> NOTICE:
> Illegal Microsoft Windows license detected!
> You are in violation of the Digital Millennium Copyright Act
> Your unauthorized license has been revoked
> For more information, please call us at:
> 1-888-NOPIRACY
> If you are outside the USA, please look up the correct contact information on our website, at:
> www.bsa.org
> Business Software Alliance
> Promoting a safe & legal online world

L'unica modificazione è l'indicazione del numero di telefono.

3. COME FUNZIONA?

Opaserv e le sue varianti si introducono nei computer attraverso Internet, utilizzando a questo fine le porte di comunicazione 137 e 139 che, normalmente, per difetto rimangono aperte. Se il computer colpito condivide file o risorse con altri computer, il codice abusivo si trasmetterà a questi ultimi servendosi di una vulnerabilità di Windows 9x e ME conosciuta come "Share Level Password". In questo modo può arrivare ad infettare rapidamente tutti i computer collegati ad una rete.
Rispetto all'Opaserv ed alle sue varianti, Luis Corrons, Direttore del Laboratorio di Ricerca sui Virus di Panda Software, sottolinea che: "questi worm stanno propiziando la rinascita di altri codici "maliziosi" più antichi, come W95/CIH o W32/Funlove. Questo fattore è dovuto", spiega," alla capacità dell'Opaserv di copiarsi nei computer che colpisce. Se questi computer sono stati contaminati da un virus, il file che contiene Opaserv sarà a sua volta contaminato e diffonderà l'infezione ovunque si propaghi."
F-Secure Corporation comunica l'apparizione in the wild del codice "malizioso" Opaserv, alias Opasoft che combina le caratteristiche di un worm di rete con le capacità di un troiano progettato per ottenere un accesso remoto non autorizzato ai computer infettati.
Opaserv si estende attraverso unità condivise di rete e si copia come ScrSvr.exe nella cartella di sistema Windows 9x, rimanendo residente nel computer contaminato. Inoltre, con l'obiettivo di essere eseguito ogni volta che si riavvii il computer, genera un'entrata nel registro di Windows.
La componente trojan di Opaserv è stata progettata per ottenere il controllo a distanza non autorizzato delle macchine che infetta. Il worm cerca di collegarsi ad un indirizzo Internet (in questo momento disattivato)
http://www.opasoft.com, per scaricare le eventuali versioni aggiornate del codice malizioso e lanciare sui sistemi catene script pericolose.
Rispetto alla sua azione diretta sull' hard disk, segnaliamo che il virus sovrascrive i due primi terzi del disco, rendendolo irrecuperabile. In base alle versioni alle quali abbiamo avuto accesso fino a questo momento, possiamo constatare che i due primi terzi vengono riscritti con codici in modo geometrico, una modalità che consente una velocità di scrittura estremamente elevata.

4. COME ELIMINARLO?

BitDefender le offre uno strumento di disinfezione imprescindibile contro il virus Win32.Worm.Opaserv.A, progettato per scoprire ed eliminare virus che hanno infettato il suo sistema. Queste applicazioni possiedono un ulteriore valore aggiunto che deriva dalle loro dimensioni, possono essere infatti scaricate facilmente persino se si possiede una connessione Internet poco potente. Si possono inoltre inviare per e-mail a clienti, amici o soci.
Se sospetta che il suo sistema possa essere stato infettato con Win32.Worm.Opaserv.A le consigliamo di scaricarlo ed eseguirlo sul suo computer. **AntiOpaserv.exe**
I servizi di Supporto Tecnico di Panda Software hanno messo gratuitamente a disposizione di tutti gli utenti che lo desiderino l'applicazione PQREMOVE, capace di rivelare la presenza di questo nuovo worm e di eliminarlo efficacemente dai computer infettati.
PER ANTIVIRUS® versione 7.8 con registro di virus aggiornato al 30 Dicembre 2002 scopre ed elimina efficacemente questo worm e tutte le sue varianti presenti e future.