

Norman SandBox

Una tecnologia esclusiva che fornisce protezione in modo innovativo

L'esclusiva tecnologia Norman SandBox consente di bloccare virus e altri software maligni ancora prima che vengano rilasciate le relative firme. La simulazione delle reti e il sistema avanzato di rilevamento dei worm Win32 consente di individuare virus sconosciuti con largo anticipo rispetto ai tradizionali antivirus e garantisce quindi un livello di protezione estremamente elevato.

Secondo un recente test condotto da AV-Test GmbH, Norman SandBox rappresenta il miglior sistema di protezione proattiva da virus nuovi e sconosciuti. Per ulteriori dettagli, visitare il sito

http://www.norman.com/News/Press_releases/17613/en

Prova sul campo

La tecnologia Norman SandBox è stata sottoposta per settimane a una serie di test di qualità in ambienti reali. In questo periodo, Norman SandBox ha bloccato diversi nuovi worm che risultavano sconosciuti.

SandBox lancia i file eseguibili sospetti all'interno di una rete informatica simulata e in questo modo fornisce una nuova linea di difesa che non si basa sugli aggiornamenti delle firme o su sistemi euristici che ricercano frammenti di codici virali noti.



Worm per e-mail a diffusione di massa - Una tecnica in ascesa

I worm che si diffondono tramite e-mail utilizzano fondamentalmente due approcci. Tentano di penetrare direttamente nei server SMTP, utilizzando le librerie WinSock o WinSock2 oppure passano attraverso la libreria MAPI.

Alcuni worm utilizzano combinazioni, quali ad esempio il recupero di indirizzi e-mail, di righe dell'oggetto o di testi reperiti tramite MAPI, per mascherare la loro presenza e diffondersi tramite SMTP. Altri si connettono a macchine „hard coded“ (mediante IP o DNS) con scopi diversi. Potrebbero aggiungere parti all'intestazione del messaggio, ad esempio facendo in modo che Outlook Express invii automaticamente gli allegati.

Vi sono molti modi con cui i worm trovano gli indirizzi e-mail: alcuni esaminano il file system alla ricerca di EML, HTML e altri file di testo che potrebbero contenere gli indirizzi. Altri controllano le impostazioni del Registro per individuare il file della Rubrica di Windows e altri ancora utilizzano la libreria WAB32 per recuperare gli indirizzi della Rubrica di Windows.

Worm che si diffondono nella rete

I virus che si diffondono attraverso le condivisioni in rete utilizzano varie tecniche per infettare i sistemi remoti. Il DLL Kernel32 contiene API che elencano le unità valide e API che aiutano a determinare il tipo di unità. Alcuni virus si replicano nell'unità oppure iniziano a esaminare il file system dell'unità fino a trovare una posizione adatta.

MPR.DLL fornisce alle applicazioni l'accesso alle funzioni WNet. Tali funzioni consentono a virus e worm di esaminare la rete in cui si trovano. Possono controllare i vari componenti, come ad esempio unità condivise, stampanti o contenitori i cui oggetti includono altre macchine. Quando un worm trova una risorsa di rete adatta allo scopo, si replica al suo interno, connettendosi oppure utilizzando i percorsi UNC.

Alcuni worm (ad esempio W32/Opaserv) sfruttano il protocollo SMB per infettare le macchine remote. Essi inviano messaggi sulla porta 137 verso una serie di sottoreti e attendono che qualche macchina risponda. Quando ciò avviene, determinano il nome delle risorse condivise, creano un nuovo thread e si connettono alla porta 139 della macchina remota per diffondere l'infezione.

Worm di reti Peer-to-Peer (P2P)

Molti worm si diffondono sfruttando i meccanismi delle reti P2P. Il modo più semplice consiste nell'inserirsi, con „nomi accattivanti“, nella directory di upload/download. Questi worm possono essere identificati osservando i valori del Registro.

Esistono molte reti P2P, ma probabilmente la più conosciuta è Kazaa.

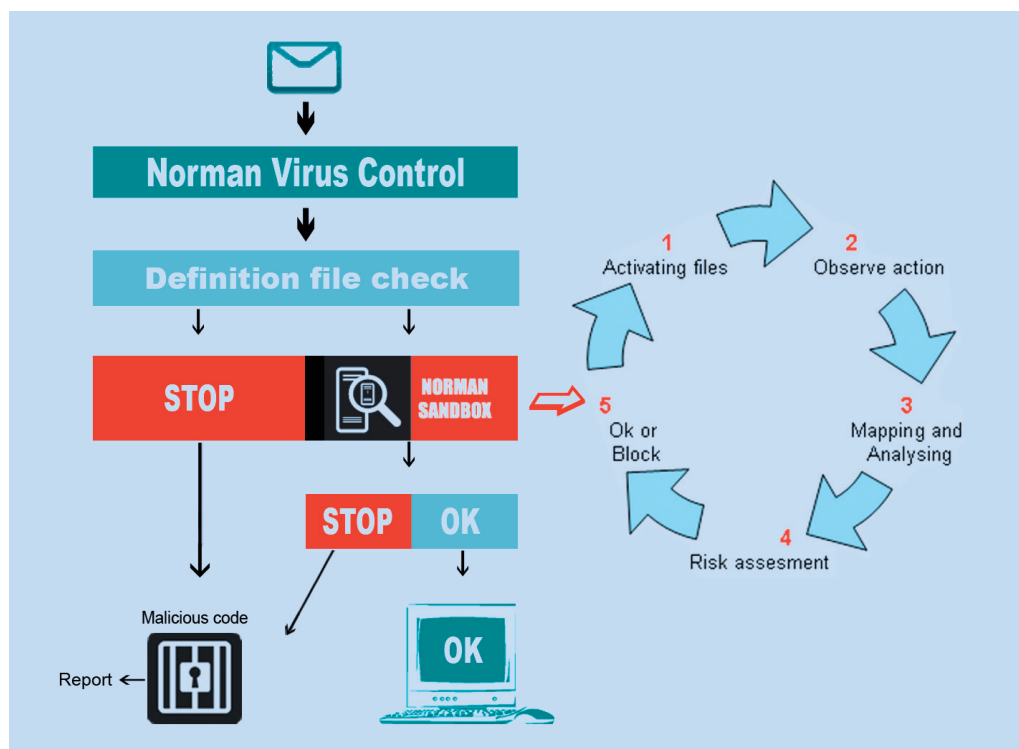
Backdoor e altri file eseguibili di tipo maligno

I backdoor sono programmi in grado di aprire porte all'interno del sistema, ponendolo in attesa di una connessione. Generalmente, consentono di eseguire attività nascoste, come ad esempio l'amministrazione remota della macchina.

Altri cavalli di troia possono utilizzare il sistema all'insaputa dell'utente per inviare dati quali comandi da tastiera, password memorizzate delle unità di rete e dialer.

Quando un file passa attraverso il controllo di Norman Virus Control, viene innanzitutto esaminato mediante il file delle firme, per determinare l'eventuale presenza di virus noti. Se non viene rilevato nessuno dei virus dell'elenco, il file viene inviato a Norman SandBox e qui rilasciato affinché possa manifestare il suo comportamento.

Se il file risulta innocuo, viene inoltrato all'applicazione che ha richiesto il controllo. In caso contrario, viene posto in quarantena per evitare che il sistema dell'utente venga infettato.



www.norman.com

Per ulteriori informazioni, visitare il sito www.norman.com/Product.

Norman soluzioni per clienti/workstation: Norman Virus Control per Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (scansione su domanda)
• Norman Internet Control per Windows 95, 98, Me, NT4.0, 2000, XP • Norman Personal Firewall • Norman Ad-Aware

Norman soluzioni per server: Norman Virus Control per Microsoft Windows NT4.0, 2000, 2003 • Norman Virus Control Firebreak per Novell Netware 4.11 e seguenti • Norman Virus Control per Linux • Norman Virus Control per OS/2

Norman soluzioni per web/gateways/mailservers: GFI MailEssentials • GFI MailSecurity • GFI DownloadSecurity • NVChet • Norman Virus Control per Lotus Domino (Win32, OS/2) • Norman Virus Control per Firewall-1 NG • Norman Virus Control per Microsoft Internet Information Server • Norman Virus Control per Microsoft Exchange • Norman Virus Control per Microsoft Exchange 5.5 • Norman Virus Control per MIMESweeper



NORMAN[®]
www.norman.com