

## **Sicurezza e controllo:**

# **l'approccio più intelligente a malware e conformità ai criteri**

La continua evoluzione delle minacce provenienti dal malware, combinata con la crescente richiesta di metodi di lavoro flessibile, costituisce una sfida notevole per i dipartimenti IT che cercano di ridurre l'assistenza agli utenti e valorizzare gli investimenti in sicurezza. Questo documento descrive i metodi attraverso i quali le organizzazioni possono beneficiare di un approccio più integrato basato su criteri per la protezione della rete a tutti i livelli, controllando sia l'accesso degli utenti che il loro comportamento.

## Sicurezza e controllo: l'approccio più intelligente a malware e conformità ai criteri

### La sfida per la sicurezza

I dipartimenti IT sono sotto costante pressione per tagliare i costi, tramite la riduzione del carico di lavoro dell'assistenza utenti e per massimizzare il ritorno sugli investimenti (ROI) nella gestione e protezione della rete. Allo stesso tempo, organizzazioni e privati si aspettano una maggiore flessibilità nei metodi di lavoro, dalle connessioni mobili e remote all'accesso web e alla messaggistica istantanea (IM). Ora l'equilibrio tra produttività e protezione della rete è in pericolo: la necessità di incrementare la produttività aziendale spinge verso una maggiore apertura della rete, che a sua volta aumenta i rischi per la sicurezza di quest'ultima.

La sfida per i dipartimenti IT consiste nel gestire la richiesta di flessibilità in un ambiente in rapido cambiamento. Le pressioni esterne includono la rapida crescita delle minacce mirate, le regolamentazioni sempre più restrittive e la verifica dei requisiti di conformità; sul fronte interno, i costi dell'assistenza utenti aumentano e la rete diventa sempre più eterogenea, con numerosi livelli di protezione, sistemi operativi e tipi di periferiche.

Le soluzioni antivirus, in particolare antispam, sono state viste come un peso eccessivo sui bilanci e sulle risorse dell'IT, soprattutto in relazione allo sforzo necessario per la risoluzione dei problemi, anche di quelli legati all'implementazione di certe soluzioni. Al fine di ottenere una protezione più efficace e migliorare il ROI, il dipartimento IT deve poter gestire non solo le minacce più ovvie, costituite da

malware e spam, ma anche l'accesso degli utenti alla rete, controllando le modalità con cui vi accedono, i computer e la protezione che usano e quali applicazioni eseguono.

### La costante minaccia del malware

Il comportamento degli utenti non controllati è solo uno degli aspetti nel panorama delle minacce. Il problema fondamentale costituito dalla rapida evoluzione del malware non è svanito. Al contrario l'evoluzione sta accelerando e diventando sempre più complessa, con attacchi sempre più mirati. La necessità di protezione multilivello non è mai stata così grande e le organizzazioni devono tutelare la rete dal gateway all'endpoint, includendo tutti i punti di accesso. La Figura n.1 mostra l'esplosione delle nuove minacce rilevate

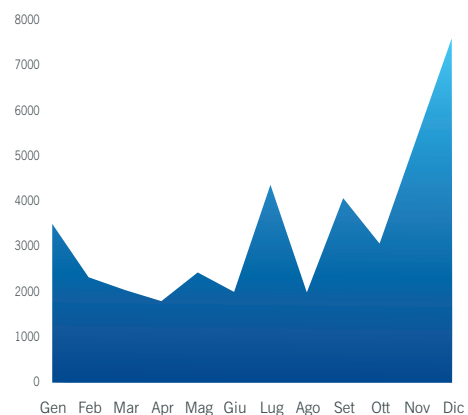


Figura 1: le nuove minacce malware in ciascun mese del 2006

da Sophos durante il 2006, che ammontano a più di 40.000. L'improvviso aumento a più di 7600 in novembre, quasi quattro volte rispetto a quanto rilevato nello stesso mese del 2005, può essere attribuito ai worm diffusi via email appartenenti alla famiglia Stratio e alle sue migliaia di varianti, che aumentano le possibilità di sfuggire al rilevamento. Sebbene questo sia stato un picco, la tendenza complessiva di crescita sembra verosimilmente continuare.

### La minaccia dal web

Il web è ora percepito dagli amministratori come la più grande minaccia alla sicurezza e alla produttività<sup>1</sup>. Non solo alcuni siti internet sono caratterizzati da contenuti palesemente non desiderabili, ma molti altri ospitano anche spyware e adware. C'è stata una crescita esplosiva delle applicazioni per il download basate sul web che contengono spyware: la Figura n.2 mostra la percentuale di email contenenti spyware e la percentuale di quelle che contengono collegamenti a siti Internet dai quali gli spyware vengono scaricati, è evidente lo spostamento della tendenza verso i programmi per il download automatico verificatosi durante il 2006.

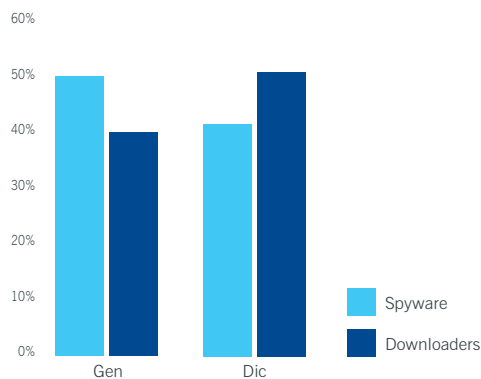


Figura 2: spyware e software di download automatico nel 2006

Secondo un sondaggio, i dipendenti passano circa il 20% del tempo trascorso su Internet per affari personali o svago<sup>2</sup>, incrementando così il rischio di scaricare inavvertitamente il malware, in particolare applicazioni per il download di spyware e Trojan. La navigazione non gestita e le transazioni via web nel posto di lavoro giocano a favore degli spammer e degli autori di malware, esponendo gli indirizzi di posta elettronica dell'azienda allo spam, alla raccolta da parte degli spammer e al phishing. Secondo un'analisi svolta dai Sophos Labs nel 2006, oltre il 75% di tutte le email di phishing avevano come obiettivo utenti di PayPal o eBay.<sup>3</sup>

Le organizzazioni necessitano di una soluzione efficace per la protezione web che non solo protegga da tutte le forme di malware, ma che elimini anche le applicazioni potenzialmente indesiderate (PUA) e prevenga automaticamente la navigazione web non autorizzata, controllando l'accesso a siti pericolosi già noti. Una soluzione simile ha bisogno di una continua analisi del traffico web in tutto il mondo, che valuti la categoria, il codice e la condotta delle pagine web.

### Le minacce provenienti dalle email

Le organizzazioni dovrebbero vigilare costantemente per tutelare i loro sistemi di messaggistica assicurando che i gateway delle email, i server del software condiviso e i database, come Lotus Domino e Microsoft Exchange, siano protetti dalle minacce derivanti dalla posta elettronica. Tuttavia, il codice malevolo viene nascosto e diffuso attraverso tecniche sempre più astute e la semplice inclusione di malware negli allegati delle email è in declino, riguardando solamente una email ogni 337 nel 2006, contro una ogni 44 nel 2005.

Sempre più spam contiene immagini incorporate, incrementando le possibilità che il messaggio venga letto e riducendo il tasso di rilevamento da parte dei filtri antispam che si affidano alla analisi del contenuto testuale. Questi file di grandi dimensioni ostruiscono le caselle di posta elettronica e possono dirigere gli utenti verso siti web che distribuiscono malware. Ad esempio, un email di spam risalente al novembre 2006 che offriva gratuitamente immagini e video espliciti, conteneva in realtà un collegamento al Trojan Psyme-DL, potenzialmente in grado di prendere il controllo del computer preso di mira. Lo spam più recente è in grado di mutare per evitare il rilevamento e spesso fa uso di reti di computer zombi per diffondersi massicciamente azzerando i rischi di inclusione nelle blacklist.

*“L'attuazione di un criterio di sicurezza su larga scala per gli endpoint sarà in grado di fornire autonomamente una protezione significativa contro i worm e gli attacchi misti, tra le minacce più importanti che le imprese devono affrontare al giorno d'oggi.”*

*Scott Crawford, Enterprise Management Associates<sup>4</sup>*

Una protezione veramente efficace è fornita dalle soluzioni in grado di identificare le campagne di spam e le famiglie di malware. Queste non si affidano esclusivamente al rilevamento di identità specifiche di virus e spam, permettendo così l'applicazione di vari criteri per soddisfare le necessita di diversi gruppi di utenti e i requisiti per la conformità.

### La minaccia per i computer endpoint

Una protezione specifica contro malware, hacker e applicazioni indesiderate per i computer desktop e per i notebook, è ancora indispensabile, come ricordato da tre ben noti worm, diffusi via email, che hanno rappresentato quasi il 40% del totale in circolazione nel novembre 2006: Stratio-Zip, Netsky-D, e MyDoom-O erano tutti in grado di essere eseguiti su Windows Vista. Tuttavia, non è più necessario gestire una varietà di prodotti per fermare differenti minacce. I migliori prodotti per la sicurezza endpoint si sono evoluti oltre la semplice protezione da spyware, virus, Trojan, worm e applicazioni potenzialmente indesiderate. Ora è possibile attuare un criterio da un'unica console centrale per gestire la protezione dalle intrusioni attraverso un client firewall, il codice malevolo prima che venga eseguito, con i vantaggi dell'Host Intrusion Protection System (HIPS) e del controllo dell'accesso alle applicazioni non autorizzate.

### Applicazioni non autorizzate

Nonostante i potenziali vantaggi per le imprese e la produttività, le applicazioni che sfruttano il Voice Over Internet Protocol (VoIP) e quelle per la messaggistica istantanea possono essere una distrazione per i dipendenti, se usate in maniera inappropriata. Il VoIP, che permette servizi di telefonia via internet e i progetti di calcolo distribuito come SETI@Home (che supporta la ricerca di intelligenze extraterrestri), sfruttano anche la capacità di calcolo residua della rete, rallentandola e incrementando inutilmente il carico di lavoro del dipartimento IT. Giochi e software di condivisione file peer-to-peer (P2P) possono inoltre causare problemi con le applicazioni aziendali legittime, danneggiando sia la produttività personale che quella dell'IT.

### Minacce emergenti

Alle normali preoccupazioni degli amministratori ora si aggiungono minacce emergenti come lo scareware e il malware per i telefoni cellulari. Lo scareware è un tipo di software progettato per ingannare gli utenti di internet, facendo loro credere che il PC è infetto o vulnerabile e spingerli così ad acquistare una versione completa del software che

disinfetterà il loro computer. Il malware per telefoni cellulari che infetta PDA e smartphone rimane un problema relativamente piccolo se confrontato con l'enorme quantità di malware che colpisce i computer Windows ma anche questa minaccia sta lentamente diventando reale e le organizzazioni devono essere preparate a implementare delle soluzioni efficaci per la sicurezza mobile.

*“Network Access Control permette agli amministratori di riprendere il controllo delle loro reti. Prima era come lasciare spalancata la porta d'ingresso della rete.”*

*Lawrence Orans, Gartner Inc<sup>5</sup>*

### Controllare il comportamento dell'utente

Sia i dipendenti remoti che gli utenti ospiti collegati in rete, possono compromettere la sicurezza se connettono periferiche non conformi alla politica dell'organizzazione riguardante applicazioni autorizzate, sul software antivirus e le patch per sistemi operativi. I rischi per la sicurezza



Figura 3: sicurezza e controllo integrati

aumentano sostanzialmente quando gli impiegati si collegano da remoto usando la tecnologia wireless oppure connettono PDA e memorie usb alla rete. Appaltatori e partner possono costituire una minaccia simile per la rete nel caso connettano computer che non sono conformi ai criteri aziendali, magari eseguendo applicazioni non autorizzate e scaricando file da internet, eventualmente senza alcun intervento o controllo.

Mentre utenti di tutti i tipi continuano a sfruttare le nuove tecnologie per lavorare in maniera più efficiente e rapida, le organizzazioni necessitano di minimizzare l'impatto che questo può avere sulla protezione della rete e sulle risorse IT, implementando criteri in grado di controllare non solo chi debba accedere alla rete e a quali parti di essa, ma anche le azioni consentite durante la connessione.

### Controllo dell'accesso alla rete

Gli analisti del settore sottolineano che l'implementazione di un controllo dell'accesso alla rete (NAC) sia essenziale al fine di mitigare i potenziali rischi posti da una forza lavoro sempre più mobile e affidata alla tecnologia, oltre che per soddisfare le normative vigenti. Il NAC autentico include la reportistica sulla conformità ai criteri di sicurezza dei computer connessi in rete, oltre all'attuazione di criteri per gestire l'accesso a diversi livelli. Il NAC permette inoltre alle organizzazioni di attuare criteri di sicurezza finora previsti solo sulla carta dalle linee guida aziendali. Sviluppando i criteri di sicurezza ad un livello sufficientemente definito per diversi gruppi di utenti, la produttività può essere mantenuta e tutti i punti della rete protetti automaticamente senza incrementare il carico di lavoro dell'assistenza agli utenti.

Inoltre, una soluzione software che mantiene e utilizza i livelli esistenti di sicurezza, non solo massimizza la continuità operativa dell'infrastruttura aziendale e semplifica l'implementazione, ma è più efficiente e aumenta il ROI. La Figura 3 riepiloga i vantaggi per gli amministratori di rete derivanti dall'uso di criteri di sicurezza integrati e un singolo agente per controllare sia il comportamento che la protezione degli utenti.

## Riepilogo

Gli strumenti di sicurezza convenzionali proteggono da singole fonti di minaccia (ad esempio antivirus o sistemi di blocco dei contenuti web) ma non sono in grado di controllare computer sconosciuti o non conformi connessi alla rete. La rete diventa sempre più aperta e le minacce sempre più variegate, le soluzioni per la sicurezza devono pertanto cambiare per controllare l'accesso e il comportamento degli utenti, piuttosto che limitarsi al rilevamento e al blocco delle minacce. Le organizzazioni possono massimizzare il loro ROI in sicurezza e controllo

implementando una soluzione basata su criteri in grado di fornire un approccio semplificato, integrato e automatizzato con un singolo agente, un sistema di controllo unico che protegge contro tutte le minacce e i comportamenti non conformi. Il controllo delle applicazioni, il controllo dell'accesso alla rete e al web diventeranno progressivamente parte di una normale gestione della protezione per organizzazioni di tutte le dimensioni, riducendo significativamente i rischi economici e migliorando la produttività del dipartimento IT ad un costo complessivo inferiore. ◆

---

## La soluzione Sophos

Sophos protegge a tutti i livelli, dal gateway all'endpoint.

**Sophos Endpoint Security** fornisce una protezione integrata contro virus, spyware, adware, PUA, e hacker prevenendo l'uso di applicazioni non autorizzate, il tutto gestito da una console centrale. Protegge inoltre da virus e spyware sulle periferiche Windows Mobile.

**Sophos NAC** blocca gli utenti non autorizzati, controlla l'accesso degli utenti ospiti e assicura che gli utenti legittimi siano conformi ai criteri di sicurezza dell'organizzazione, in modo tale che gli amministratori sappiano chi e cosa è connesso alla rete.

**Sophos gateway security** integra antivirus, antispam e l'attuazione dei criteri di sicurezza al gateway email, con un insieme di soluzioni software altamente flessibili e scalabili e di appliance email gestite. Le web appliance di Sophos proteggono il gateway web da malware e contenuti indesiderati, garantendo una navigazione sul web sicura e produttiva.

I **Sophos Labs™** sono la rete mondiale di centri di ricerca sulle minacce che analizza il traffico web e email 24 ore su 24 per fornire protezione contro minacce conosciute e sconosciute, ovunque nel mondo, indipendentemente dalla loro origine.

Per maggiori informazioni sui prodotti Sophos e su come valutarli, visitare [www.sophos.it](http://www.sophos.it)

## Fonti

- 1 Report sulla sicurezza 2007 Sophos.  
[http://www.sophos.it/security/whitepapers/sophos-security-threats-2007\\_wsrit](http://www.sophos.it/security/whitepapers/sophos-security-threats-2007_wsrit)
- 2 Burstek releases 2005 internet usage study (inglese).  
[www.findarticles.com/p/articles/mi\\_m0EIN/is\\_2006\\_March\\_20/ai\\_n16109780](http://www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780)
- 3 [www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html](http://www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html) (inglese)
- 4 Scott Crawford, Senior Analyst, Enterprise Management Associates, 2007
- 5 Lawrence Orans, Research Director, Gartner Inc

## V. anche:

(White paper Sophos) Messaggistica istantanea, VoIP, P2P e giochi sul luogo di lavoro: come riprenderne il controllo, febbraio 2007.

<http://www.sophos.it/security/whitepapers/sophos-app-control-wpit>

(White paper Sophos) Maximizing security and performance for web browsing: the challenge for SMBs, ottobre 2006.

<http://www.sophos.com/security/whitepapers/sophos-web-security-wpus> (inglese)

## Informazioni su Sophos

Sophos è società leader a livello mondiale nella sicurezza informatica e nella tecnologia di controllo dell'accesso alla rete. Sophos garantisce una protezione completa, sia a livello gateway che endpoint, contro minacce complesse quali malware noto e sconosciuto, spyware, intrusioni, applicazioni indesiderate, spam, violazioni delle politiche di sicurezza aziendale e accesso non controllato alla rete. Le soluzioni Sophos, affidabili e facili da utilizzare, sono progettate su misura per le aziende, il settore education e la Pubblica Amministrazione, e proteggono oltre 100 milioni di utenti in più di 150 Paesi. Sophos dispone di una rete mondiale di centri per l'analisi delle minacce informatiche, in cui operano esperti altamente qualificati. Forte della propria esperienza ventennale nel settore e della competenza dei propri centri di ricerca e analisi, Sophos risponde tempestivamente alle nuove minacce alla sicurezza e vanta un livello invidiabile di soddisfazione dei clienti. Sophos è una multinazionale con sede centrale a Oxford, Gran Bretagna.

Boston, USA • Magonza, Germania • Milano, Italia • Oxford, UK • Parigi, Francia  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Giappone

© Copyright 2007. Sophos Plc.

*Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari.  
Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, senza previa autorizzazione scritta del titolare dei diritti d'autore.*

**SOPHOS**  
WWW.SOPHOS.COM