SOPHOS

Safe and productive browsing in a dangerous web world: The challenge for business

With a brand new infected webpage discovered every 14 seconds, the web has now become the key vector for online hacking attacks, as well as representing a drain on productivity for many businesses. Yet the vast majority of businesses are unprotected against today's modern web-based malware. Few organizations have deployed proactive protection to combat the dangers and ensure that both network security and employee efficiency remain uncompromised. This paper highlights the six top tricks used by hackers and describes the three pillars of protection organizations need to safeguard their systems and resources.

A Sophos white paper

February 2008

Safe and productive browsing in a dangerous web world: The challenge for business

Web-based malware: the new weapon

Cybercriminals have traditionally used email as their preferred vector of attack. However, as organizations have become wise to this danger and introduced measures to protect their email systems, hackers have shifted their attentions to the still largely unprotected web, using web-based malware to steal confidential information directly or to establish botnets – networks of hijacked computers – from which spyware, viruses, spam and other threats can be distributed.

Constantly taking advantage of any new infrastructure or browsing vulnerabilities, hackers are able to post their malicious code on legitimate websites – at the beginning of 2008, webpages were being infected at the rate of 6000 a day, or one every 14 seconds.[1] Such is the scale of the problem that the second most common piece of malicious code blocked by Sophos during 2007 was Mpack, a malware creation kit for webpages freely available as an internet download.

> *One newly infected webpage is discovered every 14 seconds.*
>
> *Sophos security threat report 2008*[1]

With just 15% of businesses currently having some form of proactive threat protection at their web gateway,[2] and web browser patches very often not being kept up to date, it easy for hackers to infect thousands of systems every day via the web.

The impact of this activity is extremely lucrative for the criminals – a single compromised computer can give access to thousands of records. It is also extremely costly to businesses – estimated at 197 US dollars per compromised customer record in 2007.[3]

In addition to the significant security risks, organizations are having to deal with the adverse impact on productivity brought about by the explosion in popularity of social networking and other non-business-critical sites. Unauthorized surfing can cause network slowdown, staff inefficiency and further security (and legal) risk if sensitive company or personal data is posted online.

A new box of tricks

A number of factors combine to dictate the success or failure of a piece of malware, including how and to whom it is delivered, how it is executed, how rapidly it spreads and how successfully it evades detection. Hackers have developed a new box of tricks designed to maximize the infection rate of their malware.

TRICK ONE

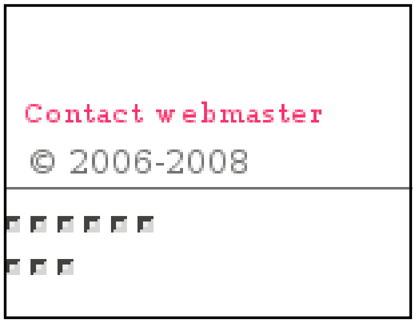
Improving reach through reputation hijacking

83 percent of all malware-infected webpages are found on completely legitimate websites.[1] The most cost- and time-efficient way for malware authors to infect computers over the web is to host their malware where the largest number of people will see it. This is exactly what they are doing when they hijack the reputation of existing websites, drawing in unsuspecting users by piggybacking on the popularity and credibility of these presumed-to-be-safe URLs.

Although hackers do also specifically create new infected websites by using free web hosting services or, more usually, by using a domain name that is similar to an existing, legitimate brand, this is a much less common practice than that of reputation hijacking.

> *83 percent of all malware-infected webpages are found on completely legitimate websites*
>
> *Sophos security threat report 2008*[1]

The <IFRAME> HTML tag, provides a very convenient mechanism for cybercriminals to infect a website and in 2007 accounted for more than 50% of web-based malware.[4] By targeting an insecure web server or by exploiting other new vulnerabilities before patches are available, hackers can quickly and easily inject numerous pages on multiple websites with a malicious iFrame. As this code is virtually or completely invisible (it can be as small as one pixel x one pixel, or can even be set to 0), content can be loaded without the knowledge of either the site administrator or the site visitor.



Contact webmaster

© 2006-2008

Webpage infected with multiple iFrames

In the example above, each of the boxes represents an iFrame with a width and height of 3 pixels. Had their width or height been set to 0, there would be no visible indication on the compromised page.

Having been unwittingly loaded, the malware is now able to execute its payload on the user's computer. This type of threat can replicate extremely quickly, to devastating effect. In China in late 2006, the parasitic Fujacks virus infected several million computers. Its rapid rate of infection was accomplished by instructing every infected computer to automatically inject a malicious iFrame to all HTML and other web files on every computer it had direct access to. This resulted in many corporate websites becoming infected through their employee's infected systems.

Concentrated efforts over long periods of time to infiltrate sites receiving a high number of visitors has led to high-profile successes for the hackers. In 2007, affected social networking sites included MySpace, Facebook and Google's Orkut, the latter infecting more than 670,000 users.[5] The Miami Dolphins' website was targeted just days before the team's stadium was due to host the Superbowl in February 2007, and infected thousands of computers.

No sector is immune from attack. Government sites, such as the US Consulate in Russia, have been infected and even the website of IT security vendor, Computer Associates, was briefly compromised with visitors being redirected to malicious content.[6] Lower profile and hobbyist websites are likewise susceptible with infected sites including Christian ministries, organic food producers, landscape gardeners, even ice cream makers.

TRICK TWO

Masking the attack with downloader disguise

Instead of placing their malicious code directly on a webpage, cybercriminals frequently place "downloaders". These Trojans are designed to bypass most defense mechanisms. They contain very little code and do not themselves have a malicious payload. Instead, once installed on a computer, they download the actual payload from another website, often via a different port. In more complex examples, the infection mechanism may involve other downloader components, which retrieve content from multiple web domains or even download malware in pieces to avoid detection, reassembling it at the endpoint. The payload can also be delayed, making it harder for users – and behavioral security technologies – to notice suspicious activity.

Numerous families of downloaders exist. Clagger, first seen in February 2007, has been so effective, it has been revised 80 times in new attacks.

TRICK THREE

Infecting silently by drive-by download

Infection by drive-by download requires nothing more than that users surf the web and visit an infected webpage using an unpatched browser. They are not tricked into clicking particular links or opening particular files. Their computer becomes infected simply because they have visited a site where known browser vulnerabilities have been exploited by a malware author.

The problem for administrators is that keeping up-to-date with browser and plug-in patches is not as straightforward as patching the operating system. There can be several browser and plug-in patches a month – all from different vendors. In just one example of the problem, in early 2008 vulnerable image upload ActiveX controls used by MySpace and Facebook left users open to attack.[7]

Often used in combination with reputation hijacking, which provides a way to reach the victim, drive-by downloads are an effective mechanism in the hacker toolkit.

TRICK FOUR

Exploiting user errors through look-alike domains

By setting up websites using domain names that are similar to those used by bona fide sites (for example, 'Goggle' instead of 'Google', or by using a '.tv' ending instead of '.com'), hackers can rely on common user errors as a simple mechanism for getting users to land on their webpages. These pages are like traps waiting to ensnare and infect unsuspecting visitors. Because these look-alike websites generally resemble the site the user had intended to visit, users can be easily tricked into opening or downloading seemingly safe content.

TRICK FIVE

Leading to malware through fast-flux spam attacks

Cybercriminals are turning away from sending malware as attachments in email messages and instead are increasingly seeding their spammed email with links to infected webpages. Behind these links are armies of infected computers, known as botnets, acting as web hosts. The malware authors cycle through these to provide a constantly changing malware-infected landing page to anyone who follows a link. This process of rapidly changing the IP address of the computer hosting the malware is known as “fast flux” and increases the difficulty for security filters to find and block the associated spam attacks.

Just as social engineering tricks have been used to encourage users to click on email attachments, the same methods are tricking them into clicking on links to webpages. The Storm (or Dorf) worm used topical news stories, e-card greetings, fake YouTube messages, and sports events to make it the most disruptive threat of 2007.

TRICK SIX

Beating security defenses through fast updating

In stark contrast to the ‘fire-and-forget’ method of email-borne viruses and worms, modern web threats are constantly being adapted and modified, in an attempt to bypass defenses. By repacking threats over and over again, hackers can create numerous minor variants, some of which may not be recognized by security solutions. This process can even be automated, allowing criminals to generate multiple malware variants in a single day.

This constant modification of code not only enables hackers to compromise more computers, it also means that, once infected, they stay infected longer than before. By continually changing the characteristics of their code, hackers can cheat signature-based malware detection engines (or those with relatively poor proactive scanning capabilities) and add more malware, such as spyware or adware to the computer. Alternatively the compromised computers could be used to launch repeated spam campaigns or distributed denial-of-service attacks.

Family	Update rate (days)
Mal/ObfJS	<1
Mal/Clagger	1.5
Mal/Dorf	1
Mal/Dropper	3
Mal/DownLdr	3.5
Troj/Pushdo	4

Source: SophosLabs

Examples of frequently updated malware families

The three pillars of modern web protection

Today's rapidly evolving web threats and the instant exploitation of any vulnerability by malware authors means that it is simply not enough for businesses to protect their email and endpoint systems. They need to act now to ensure that surfing the web at work poses no threat to IT security, to network resources or to staff productivity. In addition to good preventive practice such as rigorous patching and educating users about the risks of browsing, it is vital that organizations implement a comprehensive web security solution, comprising three key pillars of protection:

- **Reputation-based filtering**
- **Real-time predictive threat filtering**
- **Content-based filtering.**

PILLAR ONE

Reputation-based filtering

Reputation-based filters are the first critical component in the fight against web-based threats. They prevent access to a catalogue of sites that are known to have hosted malware or other unwanted content, by filtering URLs based on their reputation as "good" or "bad", and are an established and proven tool for successfully protecting against already known and located web-based threats. As well as providing this basic form of preventive protection, they help optimize network performance and staff productivity by blocking access to illegal, inappropriate or non-business-critical web content.

Although these traditional URL filters often connect to vast, regularly updated databases of sites known to host malware or suspicious content, they have one significant shortcoming – that cybercriminals are well aware of – namely that they offer no protection against malware hosted on legitimate, previously safe, sites that have become hijacked or on newly created websites. Traffic from these sites is not blocked and malware, whether new or old, is allowed into the organization.

PILLAR TWO

Real-time predictive threat filtering

Real-time predictive threat filtering goes a long way to closing the gap left by reputation-based filters. All web traffic passes through a scanner designed to identify both known and newly emerging zero-day malware. The malware engine is optimized for low-latency scanning and whenever a user accesses a website, irrespective of its reputation or category, the traffic is scanned using a combination of signatures and behavior-based technologies.

It is worth noting that this type of real-time scanning has a further advantage over traditional URL filters, in that the filtering is, almost by definition, bi-directional – both the user request to, and information returning from, the web server are scanned. In addition to detecting known malware as it moves across legitimate sites, this bi-directional filtering can also provide protection against new threats regardless of where they are hosted.

The use of real-time predictive threat filtering remains uncommon amongst many of the leading web filtering security solutions in the market today. Many security vendors are currently relying on signatures alone. Others who are fairly recent entrants to the market claim comprehensive solutions but lack the evidence to prove they are delivering fully proactive protection.

Key questions to ask a prospective vendor

- Does the URL database used for your reputation-based filtering have global coverage?
- How frequently is the URL database updated to include new threats?
- How do you identify new web threat hosts?
- How many new threat-hosting sites are identified daily?
- Can I block or allow users by webpage category?
- Can I customize browsing privileges for specific work groups or individuals?
- Can I set time-based policies to restrict surfing of “leisure” sites to certain times?
- Do you scan all incoming traffic for malware?
- Do you analyze the true content of files, or rely on the extension or the MIME-type?
- Do you use your own technology for malware scanning or rely on or third-parties?
- What is the performance impact of your overall solution?
- Is there an additional cost for real-time threat filtering?
- Can you demonstrate real research expertise in web threats?
- Do you have independent statistics of your proactive web threat detection rates?
- Can I see a demo of the admin console to see how easy it is to use?
- Are there on-board monitors to track software, hardware and traffic health?
- How are issues reported to the administrator? Via email? Via phone call?
- Do you provide real-time uptime monitoring to assure the system is available 24/7?

PILLAR THREE

Content-based filtering

Content-based filtering analyzes all web traffic on the network to determine the true filetype of content coming back from a website and can allow or disallow this traffic, based on corporate policy.

Content filters scan the actual content of a file, rather than simply looking at the file extension or the MIME-type reported by the web server, and so can identify and block files that are masquerading as innocent/allowed filetypes but really contain unauthorized content. A file might, for example, have a .TXT extension but in fact be an executable file.

By enabling enforcement of only business-type content, this pillar of protection enables organizations to create policies around a variety of content types that can be used to send malware, thereby reducing the risks of infection. For example Windows executables or screensavers might be disallowed. Content-based filtering also improves bandwidth optimization by blocking large or resource-hungry content, such as streaming video.

User education as a tool for defense

Many businesses have successfully educated users about how to spot email-borne threats, and while the fight against web-based threats relies much more heavily on sophisticated technology, users can and should be engaged in the fight.

Many firms already have procedures in place that define which websites are considered appropriate, but few have updated these to include guidance on how to avoid infection whilst surfing the net. A good policy will dictate that:

- Employees must never open spam emails
- Employees must never click on links included in emails sent from unknown senders
- IT must ensure that the organization's web browsers are patched at all times
- Employees should minimize their non-work-related browsing for both security and productivity reasons.

Users can also be encouraged or required to report unusual behavior, such as their computer suddenly becoming slow, or the homepage changing when they open their browser with no input from them, or they open a file that does nothing.

Conclusion

Every minute of every day, cybercriminals are looking to exploit web traffic for commercial gain, and since web browsing is integral to most businesses' day-to-day activities, it must be afforded the same level of protection as the email gateway and endpoint. Organizations looking to protect against the growing threat of web-based malware need a solution that above all demonstrates its security attributes and combines powerful site and content controls with low-impact, effective administration. At the same time end-user expectations and requirements for speed and efficiency must be met. Solutions which fail to meet these demands for security, control and performance will ultimately fail the organization.

Sophos solution

The Sophos Web Appliance, part of Web Security and Control, protects against spyware, adware, viruses, malicious code, unwanted applications and undesirable content. It features an innovative, full-spectrum scanning engine that detects all threats through a unique combination of reputation-based filtering, real-time predictive threat filtering, and content-based filtering. Its easy-to-use management console and powerful reporting tools that deliver rapid insight into web traffic, threats and user behavior, enable secure browsing without the complexity of traditional web filters. As a managed appliance, the Sophos Web Appliance features remote "heartbeat" monitoring and on-demand remote assistance, ensuring it delivers the most dependable web security in the industry.

Sources

1 Sophos security threat report, 2008
www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-report-08.pdf

2 Marketscope for URL filtering 2006. Lawrence Orans and Arabella Hallawell. Gartner, Inc. March 2006

3 2007 Annual Study: Cost of a Data Breach – Ponemon Institute, November 2007

4 Modern web attacks, Sophos Labs technical paper, Fraser Howard
www.sophos.com/security/technical-papers/modern_web_attacks.pdf

5 www.sophos.com/security/blog/2007/12/900.html

6 www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9055599

7 www.theregister.co.uk/2008/02/01/myspace_image_uploader_bug/

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.COM