

GFI WHITE PAPER

WEB-BASED SECURITY THREATS

How attacks have shifted and what to do about it

As email and web technologies converge, the number of security threats has grown, both in terms of creativity and effectiveness. Web-based threats are proving to be a nightmare for IT administrators and computer users. Although technology helps to counter these threats, a more holistic approach is needed, one that includes strict and enforceable policies as well as a proper awareness program.

From email to web

When the masses started communicating using the Internet, particularly with email, mass mailing computer worms began to do the rounds. One of the first email worms of note was called Melissa and which spread to and via a large number of email addresses. In the beginning, they were not written with any malicious intent and their impact on mail servers was such that the infrastructure often struggled to handle the load of unwanted emails.

The 'success' in terms of Melissa's ability to spread soon attracted the attention of cybercriminals who started using email worms for their own evil deeds.

By 2004, email was saturated with spam (unsolicited commercial email) and malware¹. Also by that time, a large number of end-users who depended on email had learnt valuable lessons in email security – you should not click on email attachments you were not expecting, especially those containing executable code. It was not just user awareness that changed. Many systems administrators installed email content filtering software on their email server thus cutting down on the volume of spam reaching end-user mailboxes and filtering out rogue emails and phishing attempts.

Change of strategy

As the cat-and-mouse game between the bad guys and security experts progressed, cybercriminals changed their strategy – email still proves to be a winner but changing realities and developments in web technology provided an even juicier target and more lucrative opportunities to defraud and make money – the Internet.

Anyone, including people with malicious intentions, can put up a web page that is instantly accessible by thousands of people. Instead of using email, attackers simply put their malicious content on a website. This way, they solved two difficulties: the need to make it through email defense systems and the need to convince the end-user to open the malicious content.

For online criminals, this shift from email to the web meant they could continue their illegal activities as well as target a much larger audience. At the same time, system administrators and end-users struggled to keep up. While limiting exposure to attack through email is quite straightforward nowadays, the same cannot be said about securing the web. Corporate email usually passes through the organization's email servers, thus it can be easily managed. Additionally, unlike the web, email is not necessarily instant and can be delayed for a couple of seconds while an antivirus or anti-spam program scans and filters the email. For home users, popular services such as Gmail and Hotmail have had security features, such as virus scanning and spam filtering, for quite a while. The web, on the other hand, remains relatively untamed.

Take a typical case scenario: a new employee called George was given a fresh installation of Windows with the task of researching a new software technology. While his email was being filtered for malicious content, his web browsing was not. To do his job, he needed to have unfettered access to the Internet. As part of his research, it helped that he could download software and try it before including it in his report. By the end of this exercise, his computer started playing up. After investigation, IT administrators found out that one of the downloaded software packages was in-fact trojan horse software, i.e. malicious software bundled with or marked as useful software.

The victim's computer may have had an antivirus solution installed, yet it would not have necessarily prevented malware from entering the system. The malicious software was only found because the computer stopped working properly. In a way, malware is typically discovered because it is written by sloppy programmers, it is not optimized and does not successfully hide itself. However, not all malware is noisy and therefore some malicious software may remain undetected for months, even years. In the case of George's organization, further investigation showed that more than one computer had been infected with malware.

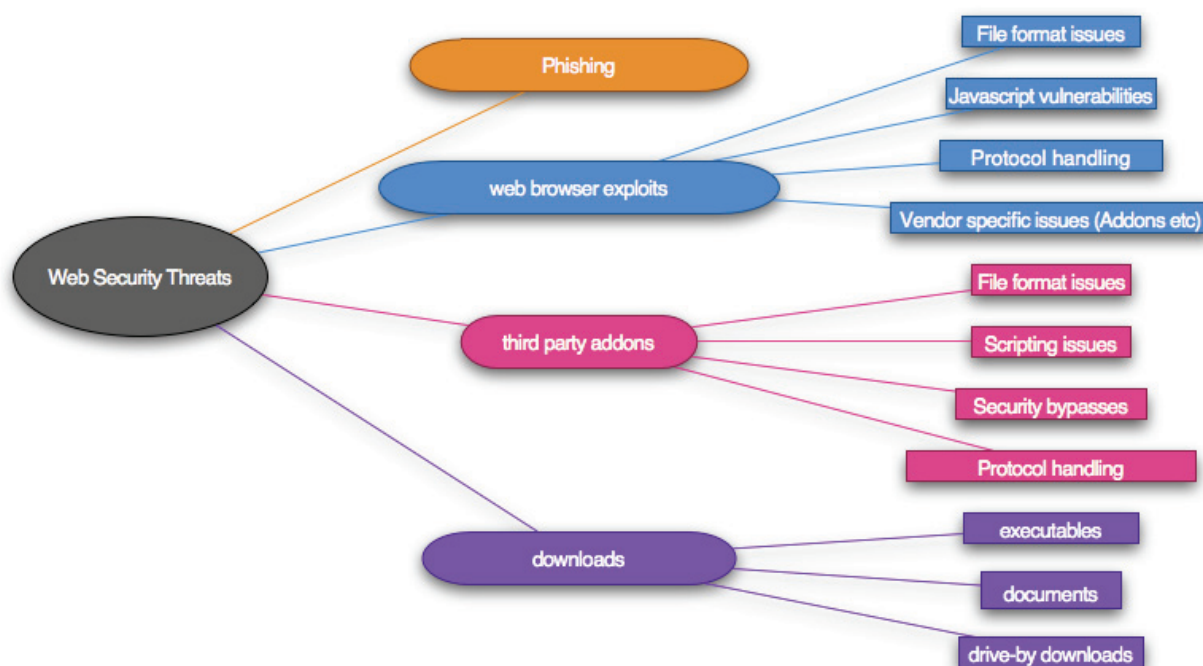
Web threats

It is not so hard to fall victim to a user account or system compromise introduced through the web. But what are the various issues involved?

Phishing

One of the less advanced, but nonetheless effective threats is phishing. The term refers to attacks where the victim is led to believe that he or she is on a legitimate website, when in fact it is just a copy of the real one. This attack relies on the fact that anyone can create their own website and any website can look like any other. A real world example would be a fake ATM that is put in the middle of a busy shopping center. There would be very few signs to show victims that it is not a real ATM – until no money comes out. Similarly, in a phishing attack victims may think that they are on their bank's website, and therefore do not think twice about using pin numbers as requested. This attack is not limited to banking systems.

If the title of the case study is short it has to be on the bottom line only. To do this, one has to write the title normally. Then put the cursor in front of the first letter of the title and press the 'Shift' and 'Enter' keys together so the title will move to the second line.



Phishing attacks have been known to target company email websites (Webmail), public email websites (like Gmail) and popular sites like Amazon or eBay.

Users can identify a phishing website in a number of ways. The first is to look at the URL. Another effective prevention technique is to never follow links by email but to type them in or use bookmarks. Although not foolproof, these methods make it harder for attackers to pull off the scam.

Web browser exploits

Cybercriminals have also set up websites that exploit security holes in the web browser. This technique allows them to gain access without the victim's knowledge. Web browsers are complex software. They have to handle various file formats, such as images, sound and HTML, Javascript and a multitude of other technologies. All of these features add to the attack surface of the web browser, thus making the technology relatively weak from a security standpoint. Yet this same functionality is what makes it so useful.

Not surprisingly, both Internet Explorer and Firefox have had their fair share of security vulnerabilities. In fact, as of 2009, Secunia estimates that Internet Explorer 7 had over 90 vulnerabilities², while Firefox 3.0 had over 130 vulnerabilities³. Some of these security flaws could be exploited to allow individuals to remotely compromise that user account. This typically means that a successful attacker who exploits the web browser gets access to private emails, sensitive documents and anything else that the user running the web browser has access to.

Third party add-ons

The majority of websites require the use of third party add-ons such as Adobe Flash player and Acrobat Reader. Both of these widely used products have become a favorite target for cybercriminals. As more administrators and home users update their machines with the latest security updates and patches for their browsers, as well as the ability to automate the process, it becomes harder to use web browsers as an attack vector.

However, although they may be updating their browser software, it is also true that many people forget to update third party add-ons like the Flash player. In 2009 a number of malware "in the wild" (out there on the Internet) have exploited the PDF file format, Adobe Acrobat, Flash, a number of ActiveX components and Java. These third party add-ons are used to push users to other websites that have been compromised.

Downloads

While automating remote code execution is very attractive for attackers, there are many times when this level of sophistication is not required to compromise end-users' computers. In fact, some attacks still rely on end-users downloading executable files. To aid attackers, legitimate websites, some of which are high profile, are being compromised. As soon as these sites become infected, they can start serving malware, thus exploiting a user's tendency to trust content based on reputation. When a legitimate news site asks end-users to download an executable file (eg. codec) to view an intriguing video, many will comply because they trust that website.

Malware creators use a variety of techniques to convince users to visit poisoned sites, search results and download executables.

The bad guys love to play on two characteristics of human nature: fear and curiosity. In 2009, the rise of 'scareware' has been considerable. Playing on people's fears that their machine has been infected with malware, users are encouraged to download antivirus software. This is nothing but malware that infects the machine and demands payment if the user wants to uninstall the software.

Another threat is the use of poisoned search engine results. The bad guys create numerous websites for well known keywords and use these sites to feature high upon on web searches. When a user searches for a particular name or subject and clicks on a poisoned link, he or she is taken to a fake website where they are told to either download software to continue or else malware is downloaded while they are looking at the content.

Hybrid attack

While the web offers much greater scope for attackers, email still remains a powerful tool. Combined with the web, the threats not only multiply but the risk that the user becomes a willing prey is very high. One common trick is to use current news events to spread malware spam. Emails purporting to offer exclusive news, videos or files are popular online traps to open dangerous attachments or be redirected to infected or fake websites.

What do these web threats lead to?

Malware infections cause a number of problems. Machines become unresponsive or sluggish resulting in users become frustrated and administrators spending precious time trying to find the problem. When a machine is infected, some administrators often want to simply re-install the operating system, however a responsible system administrator or security analyst would want to investigate and assess the situation before doing anything else. All of these tasks take time and resources. People have to stop working, the hardware has to be replaced and so on. Additionally, some malware creates a denial of service by design, increasing the possibility of an attack on the organization's infrastructure.

While most organizations understand denial of service very well – since it impacts productivity – many ignore the impact on confidentiality and integrity. Attackers are known to harvest sensitive information from compromised computers to carry out further and deeper attacks within the network. If they access the organization's data they can use this to sell to third parties and make a profit. Modern malware can create an automated process to harvest information from a network that has been breached.

Once an attacker is on the inside, his or her work is significantly easier since on most networks, systems on the inside are trusted. This is what makes attacking web visitors through infected websites so attractive to the bad guys. End-users and their web browsers are already on the internal network. Unlike traditional network-based attacks, the victim connects to the attacker instead of the other way round. Even today, most defenses are still focused on preventing attackers from trying to connect to the victim, i.e. protecting the perimeter.

What needs to be done

Prevention is certainly better than having to clean up after a security breach or web-based attack. Attacks often depend on the end-user making a mistake and clicking on attachments or links. That is why security awareness and education play an important part in the overall security of an organization's network.

If end-users are aware of the threats, understand how their actions could be a contributing factor and have clear steps to follow if they see something suspicious, then the chances are that security will improve.

Security policies

Education alone is not enough. Organizations need security and user policies that can be enforced. These policies need to be reasonable and allow employees to do their job yet limiting actions that could be a security risk. This is easier said than done because many security policies and solutions impact usability. Therefore a good security analyst has a tough job finding a balance between security and helping employees to deliver and be productive. When policies are too strong, employees will find ways around the policies or become less productive – a situation that is untenable and unacceptable for a business.

Security policies are important but only effective when they are enforced and users are aware of them. It is highly recommended that businesses create acceptable user policies that every employee has to sign. Enforcement, however, is another story and requires more than just an employee's signature on a piece of paper that they will probably never see again. Technology is key here because it allows administrators to enforce policies across the network with minimal effort.

Using technology

Although administrators are comfortable working with technology, they are somewhat limited in dealing with human nature. Policies and education are important but you will still find people who don't really care. If they want to open a file or click on a link they will do so. So administrators need to boost their arsenal with technology.

Anti-spam and anti-phishing software, for example, will reduce the volume of unwanted email reaching the end-user, thereby reducing the risk of exposure to phishing scams and redirects in email. An administrator cannot (and should not) depend on end-users to follow policies to the letter.

Bandwidth monitoring is one of the basic methods used to detect unwanted web traffic. If, on average, an employee only browses a few websites every day, but this behaviour changes drastically, the administrator needs to look into the matter. The employees may have changed his or her browsing habits but it may also be a sign that the machine has been compromised. Bandwidth monitoring is an important tool for network and security administrators.

Content filtering

While bandwidth monitoring gives an overall view of what is happening, it does not provide an in-depth analysis. Content filtering solutions for the web allow administrators to choose web content by file type and by location. Since certain file types available on the web are used more often by the bad guys, content filtering by file type is a very effective way to protect web browsers without impacting negatively

on usability. This type of solution, for example, could be used to block web content that may execute on the client, such as exe files or installation files (MSI).

Content filtering does not solve all security problems associated with web clients. In fact, malicious attackers make use of file types or web locations that are more often than not also used for legitimate purposes. For example, HTML does not typically include any malicious content. By embedding exploit code in HTML files, attackers typically bypass most content filtering that relies on blocking specific file types. Therefore having an antivirus solution – preferably deploying multiple antivirus engines – is still very effective, especially if that antivirus solution is good at catching this type of malicious content. Implementing an antivirus solution at a strategic point such as a web gateway or proxy has various advantages. It can be centrally managed and is separate from the end-user's computer that may be already infected.

Prevention is only part of a holistic solution that should be in place to counter web-based threats. Regular monitoring and auditing will help detect security incidents that may have occurred. One reason why some security incidents are more serious than they should be is that these incidents are not handled correctly. In the case of web threats, an incident response plan typically covers things like roles and responsibilities as well as procedures on how to respond to incidents with guidelines on preparation, identification, containment and recovery.

Conclusion

Web threats can affect any organization that is connected to the Internet. There is no single technology solution that addresses all concerns or that provides total security. However, a combination of software/hardware, security policies and education will provide an organization with the ability to fight off web-based threats and lower the chances of a successful attack.

© 2010. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

¹ Malware stands for Malicious software, which includes computer viruses and worms

² Vulnerability Report: Microsoft Internet Explorer 7.x - <http://secunia.com/advisories/product/12366/>

³ Vulnerability Report: Mozilla Firefox 3.0.x - <http://secunia.com/advisories/product/19089/>