INFOTECH

A guide to Web Protection: Taking a user-focused approach to network security

INFOTECH

Table of contents

Introduction

Cyber crime is one of the most innovative businesses in existence today – and make no mistake, it is a business. Cyber criminals are constantly evolving their attack techniques and tools, as cyber security researchers do their best to thwart them. In some ways, you could say that innovation is a core competency in the cyber crime world; perhaps more so even than in legitimate software development.

Cyber criminals have used the same techniques for years to infect potential victims. Those techniques are still productive, but they are increasingly moving to web-based attack vectors. They are making this transition because the cyber security industry is getting better at blocking traditional attacks, but also because web-based threats offer more opportunities to infect a computer.

Web protection systems offer businesses' a way to protect themselves against a broad range of attacks using the web as a delivery mechanism.

How is cyber crime evolving?

1 Cyber crime patterns

For years, email was the primary route for cyber criminals to enter your business and wreak havoc. Attackers would deliver malware via email, as attachments designed to tempt victims into opening them.

These techniques still represent the majority of cyber attacks on an organization, but things are changing. According to Verizon's Data Breach Investigation Report 2015, four in every 10 attacks arrived via an attachment sent in an email[1] However, the landsape is shifting, as attackers are using emails to deliver other exploits that traditional antivirus software might not see.

37.4%

OF ATTACKS WERE DELIVERED VIA A MALICIOUS LINK SENT IN AN EMAIL

According to the Verizon report, 37.4% of attacks were delivered via a malicious link sent in an email. Typically, criminals use exploit kits to infect the computers that send these emails. The exploit kits will find weaknesses in the victim's computer, and then use them to inject malicious code, compromising the machine and giving the cybercriminal control over various functions.

The infected computer is often then co-opted to send out large amounts of spam, which will typically contain links to a hosted web server that the spammer has either set up themselves, or infected. The 'bait' that persuades victims to visit those links varies, but it can include:

- **Phony customer service emails**
- **Fake delivery tracking notices**
- **Phishing content**
- **The promise of salacious material**

16.6%

OF INFECTIONS ARE DRIVE-BY DOWNLOADS

Another 16.6% of infections – an unusually strong number, according to Verizon – were delivered via 'drive-by downloads'. These occur when websites use JavaScript to exploit vulnerabilities in browser software, installing malicious code on the user's machine.

This indicates that attack vectors are beginning to shift. Aside from the fact that companies are simply getting better at spotting and blocking malicious attachments, there is another benefit to attackers of using links rather than malicious files: the browser.

Browsers interact with computers far more than email programs do. Users frequently populate them with a variety of third-party plug-ins to add extra functionality. This creates a broader attack surface for the browser, making it a particularly appealing target for malicious actors.

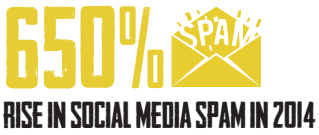
228%

INCREASE IN ATTACKS ON MICROSOFT'S SILVERLIGHT BROWSER PLUGIN BETWEEN DEC 2012 AND SEPT 2014

One example is Microsoft's Silverlight – essentially an alternative to Flash that offers multimedia capabilities in the browser. According to Cisco's 2015 Annual Security Report, this suffered an increase of 228% in attacks between Dec 2012 and Sept 2014[2].

A rising tide of malicious links

How are these bad actors delivering the links that get victims' browsers in front of their malicious code? As the digital landscape evolves, malicious links can be found in an increasingly varied number of places. Unwitting users can be presented with links to websites that will compromise their machines, in places including the following:



Social media

Social media malware is on the rise. Security firm Proofpoint found a 650% increase in social media-based spam in 2014, and predicts a further 400% increase in 2015[3].

How does it work? One example came in January 2015, when over 100,000 Facebook users were tricked into downloading malware via a link shared with them via their friends' accounts. The link offered a pornographic video, which began to play, but stopped half way through, asking users to download a video player to continue watching. The player compromised the victim's computer, and posted itself as a link on their own Facebook profile, tagging their friends[4] .

Web site visits

Websites may themselves contain links to other malicious domains. This can be a particular problem with user-generated content. Websites that allow users to post their own material online run the risk of exposing other users to malicious links.

This can be a problem in online discussion forums, or the comment sections of blogs, for example.

Instant messaging clients

Instant messaging clients are a fruitful way for attackers to spread malicious links. They will often pose as attractive women, inviting victims to chat or even watch a video, and deceive them into clicking on links in the process. Alternatively, Skype worms can be used to make infected machines send links via Skype messages, pointing to copies of their malware[5].

Malvertising

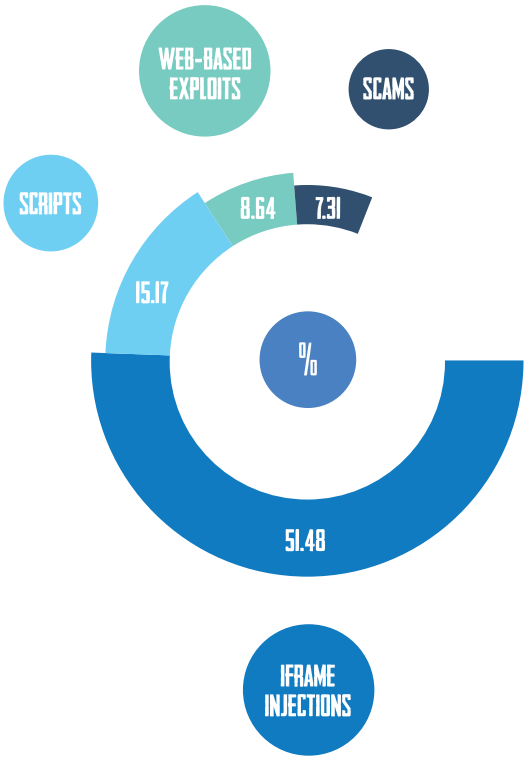
Online advertising has become a popular way to spread malicious software. Online advertising networks connect advertisers with suitable websites to clients with online commercials that they would like to display. They will typically create a space on a website, in collaboration with its owner, which can be used to serve up appropriate advertisements from different advertisers, in exchange for a fee. The ad network then takes money from its own customers to display their advertisements on its partner websites.

The problem for visitors to those websites is that occasionally, an advertising customer deliberately creates an advertisement with malicious code, effectively turning the partner website into an infection vector for visitors.

In 2013, malvertising was responsible for 209,000 malicious advertising incidents, generating over 12.4 billion malicious ad impressions, say industry estimates[6]. The problem is bad enough that the US Senate issued a report in 2014 addressing the issue[7].

Delivering malware via the web

Web-based malware can be delivered using a variety of technical measures. According to Cisco, web-based malware delivery in Europe was delivered in the following ways during 2014:



Where have we been successful so far?

2

The cyber security industry has a long history of thwarting online criminals by analyzing and countering their exploits.

Microsoft and others have continually refined their approach to scanning emails for hostile attachments, and they have also become adept at sandboxing attachments when opened to analyze their activities and determine the level of risk associated with them.

Responsible cyber security professionals in end-user companies have succeeded in reducing the likelihood of a successful attack using a variety of technologies:

- **Mail filtering**
  Anti-spam solutions have helped to stem the growing tide of spam email threatening most organizations. Using combinations of blacklists, email signature recognition, and heuristics, cloud-based providers are able to block out many potential sources of attack.

- **Antivirus**
  Antivirus technology has evolved since the late 1980s, with a variety of techniques designed to stop malicious files infecting the host machine with executable code.

- **Patch management**
  Effective patch management processes have helped to protect corporate computers from infection over the years, and companies that implement these processes properly can reduce the risk of compromise. Because infections typically rely on security flaws in operating system and application software, applying the latest bug fix updates can make it more difficult for attackers to succeed.

- **Network monitoring**
  Should an attacker succeed in compromising computers on the corporate network, network monitoring can help to spot anomalous behavior. Intrusion detection systems can watch for traffic on the network that indicates a sign of compromise, such as particular devices attempting to communicate with large numbers of other devices at once, for example.

3 What is needed next?

These successes have provided more protection for corporate networks, but they don't provide enough. In fact, it could be argued that there is never enough protection, because security is not a zero-sum game. No side in the security battle will ever entirely win. Instead, they simply gain temporary advantages as they innovate.

The gains that security professionals have already made are laudable, but corporate networks are still susceptible to attack. Mail filtering will stop the bulk of malicious communications. A new piece of malware may still infect a machine if antivirus scanners have not been updated to spot it. Patch management mitigates the risk of infection, but it won't protect users against zero-day exploits that have been carefully harbored by attackers without a vendor's knowledge.

Moreover, drive-by downloads are still an issue. If an employee surfing the web happens to stumble across a malicious website without having ever clicked on an email link, then how can an organization protect itself from their machine – and the rest of the network – being infected? Welcome to the world of web protection.

What is web protection?

4

Web protection is the final layer of defense for companies concerned about the safety and integrity of their network, and the computers running on them. Rather than monitoring the files downloaded and installed by employees, it monitors web traffic to understand where they are going, and what potential risks they face along the way. Web protection solutions actively prevent users from placing themselves in danger, thus helping to protect corporate infrastructure.

How does it work?

Web protection solutions monitor HTTP traffic passing through a central gateway. This traffic includes the web address or IP address of the browser's destination. The web protection gateway compares online destinations with websites defined in whitelists and blacklists by MSPs and their clients, to determine whether an online destination is dangerous or not.

Policies can then be set outlining the permissions to visit certain websites. In many cases, they can define these policies at a granular level, carving them up by time of day and by specific user groups, for example.

The case for web protection?

5 Why might a company decide to install web protection? It can protect against two broad categories of threat.

Deliberate employee actions

The first threat category concerns deliberate employee actions. Employees are human, and therefore don't always behave as they should. There have been cases of employees visiting inappropriate websites, including pornographic sites, that incur several risks.

These risks relate not only to legal and human resources issues (other staff will find these activities offensive and may sue for sexual harassment, for example), but also to cyber security. The more controversial the material on a website, the more likely it is to be seeded with malware.

Even if employees aren't risking infection or legal issues by visiting inappropriate sites, they may still be damaging productivity by visiting sites that distract them from their work. Social media sites are one example, as are sports sites, or entertainment destinations such as YouTube.

Unwitting compromise

Employees may visit websites that put themselves and the company in danger unwittingly, in the course of legitimate activity. Even a visit to a popular news site to catch up on issues relevant to the business can land employees in trouble. Increasingly these days, thanks to a mixture of SQL injection, flash exploits and malvertising, even sites with solid online reputations can go bad. In February 2015, hackers attacked the popular business site Forbes.com, launching a 'watering hole' attack designed to infect anyone that visited it. It used a previously patched Adobe vulnerability, along with a Zero-Day attack on Internet Explorer that Microsoft subsequently patched. Forbes is the 61st most popular website on the Internet, meaning that large numbers of web users would have been hit[8].

Benefits of web protection

Implementing web protection can provide companies with valuable benefits in several key areas.

Constant updates

The web is a fast-moving place, with new threats emerging on a minute-by-minute basis. Simply keeping track of a handful of well-known porn sites, social media networks, and sports/entertainment sites and blocking them with a firewall won't be enough to protect users from visiting the wrong places online. Web protection provides a constantly updated list of risky online neighborhoods, which can be accessed automatically by the corporate gateway. It can then block any attempt to visit sites that present a threat to the corporate infrastructure.

Policy definition

IT administrators need fine-grain controls to strike a balance between protecting the organization, and making it easy for users to do their jobs. Web protection systems with sophisticated policy definition and management interfaces make it easier for them to walk this line.

What makes for good web protection?

6 Bandwidth management

Even if online destinations do not present a security risk, business leaders may still want to know about their potential drain on resources. Streaming sites, for example, can take their toll on network bandwidth, and could slow productivity for other users. Bob in accounting may love watching the BBC World Service live video stream, but that doesn't mean he should be allowed to do it all day.

Alerting

The best web protection systems are active, providing management or IT staff with alerts when they detect specific activities online. These alerts may indicate employee misbehaviour (such as visiting inappropriate sites deliberately), but they may also tip off security professionals that a compromise is already underway. For example, if a particular workstation is trying to access an obscure Russian IP address repeatedly at 4am, there could be something amiss. Without a web protection system to alert you, would you know about it?

Use it as part of a layered defense strategy

No single security solution stands alone. Implement web protection as part of a layered defense mechanism incorporating other levels of protection. These will include:

- **Patch management**
- **Antivirus**
- **Network monitoring**
- **Email filtering**
- **Remote workstation control**

These measures will help to create a 'defense in depth' strategy that minimizes your risk of compromise.

Server protection

Workstations are a key infection vector for drive-by downloads and other malicious web deliverables, but don't forget your servers. Servers shouldn't be surfing the Internet. If they are, something is probably amiss. Put web protection on your server equipment to look for indicators of compromise.

Walk the line with employees

Employees who feel restricted at work may start to lose morale or resent management, perhaps even resorting to mobile devices to surf the online destinations they want. Avoid a punitive, totalitarian regime. Instead, use web protection wisely. Negotiate with users to give them some autonomy online. Perhaps social media sites could be allowed during lunch breaks, for example?

Combine these negotiations with employee security awareness training, so that they understand why web protection is being implemented. Align your security values with theirs. Get them on board.

Conclusion: A stitch in time

7

Given the increasing risk of web-based compromise, relying only on email filtering and software patching for protection renders organizations susceptible to risk. Cyber security is an exercise in risk management, in which the probability and impact of a risk must be weighed against the cost of avoiding it. Web protection doesn't have to cost the earth.

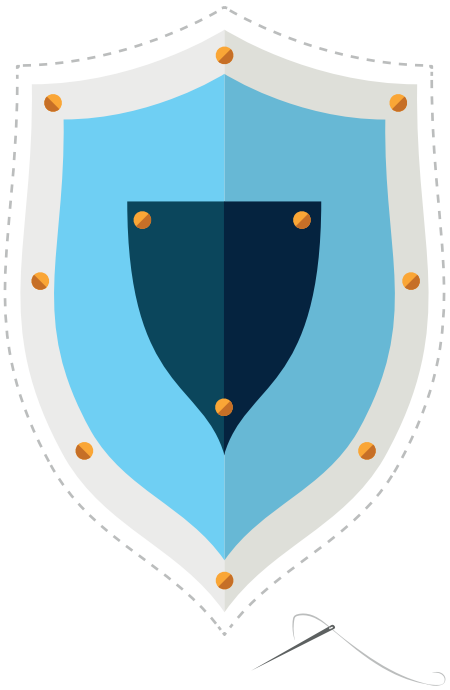
Yet the signs are that more companies could be using web protection as part of their arsenal. Cisco's 2015 security report found that only 56% of security professionals said they were using the technology in 2014. Clearly, there is room for further adoption.

Cloud-based web protection services offer a central point of security without the need to invest in hardware or software. For a few tens of dollars per client device, companies may consider this a form of lowcost insurance to prevent an incident that could give attackers a foothold on the corporate network.

Consider the cost to the business not only of losing a computer, but also of the service call involved, and the loss to productivity while the employee waits for a repair. The data that could be stolen from your company could cost a lot more than that.

It's better, surely, to invest a little money now, and save significant headaches in the future.

56% OF SECURITY PROFESSIONALS SAID THEY WERE USING WEB PROTECTION TECHNOLOGY IN 2014



Source

1 http://www.verizonenterprise.com/DBIR/2015/

2 http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf

3 https://www.proofpoint.com/us/threat-insight/post/Cybersecurity-Predictions-2015

4 http://www.itpro.co.uk/malware/23963/porn-video-malware-infects-110000-facebook-users

5 http://www.cyberoam.com/blog/skype-delivers-a-new-variant-ofmalware-yet-again-a-new-sample-of-dorkbot-worm-detected/

6 https://otalliance.org/news-events/newsletters/may-15-2014-online-trust-alliance-us-senate-testimony-malvertising-jumped

7 http://www.hsgac.senate.gov/download/?id=2A2D6AD9-77A6-43D3-B47D-C6797EA421DE

8 http://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-