Commissioned Study

SURVEY:

Web Threats Expose Businesses to Data Loss

WEBROOT®

Introduction

Web-borne attacks are on the rise as cybercriminals and others who do harm to computer systems for profit or malice prey on the Web's areas of vulnerability, and businesses are feeling the effects of the attacks on their resources. Currently the weakest link is the Web browser. Vulnerabilities in browser add-ons like Java, Flash and Adobe represent a common source of network incursions and endpoint infections. To mitigate these significant business risks a properly layered defense with effective endpoint and Web security and monitoring needs to be in place.

Webroot recently conducted research to assess the state of the Web security layer in organizations throughout the United States and the United Kingdom. The study—which focused on companies that currently have a Web security solution or plan to deploy one in 2013—found that Web-borne attacks are impacting businesses, with the majority of them reporting significant impacts in the form of increased help desk time, reduced employee productivity and disruption of business activities.

8 in 10 companies experienced Web-borne attacks in 2012.

Crucial for commerce, communication and information, the Internet is a tool that businesses must vigilantly protect from malicious attacks. Few companies avoid them altogether. In fact, the majority of companies surveyed experienced one or more types of Web-borne attacks in 2012. Businesses are taking the risk seriously; almost all Web security decision-makers agree that Web browsing is a serious malware risk to their organization.

Key Findings

- 8 in 10 companies experienced one or more kinds of Web-borne attacks in 2012.
- 88% of Web security administrators say Web browsing is a serious malware risk to their firm.
- Phishing is the most prevalent Web-borne attack, affecting 55% of companies.
- Web security administrators report that Web-borne attacks have a significant negative impact on help desk time, IT resources, employee productivity and the security of customer data.
- Companies that deploy a Web security solution are far less likely to be victims of password hacking, SQL injection attacks, social engineering attacks and Web site compromises.

Study Overview

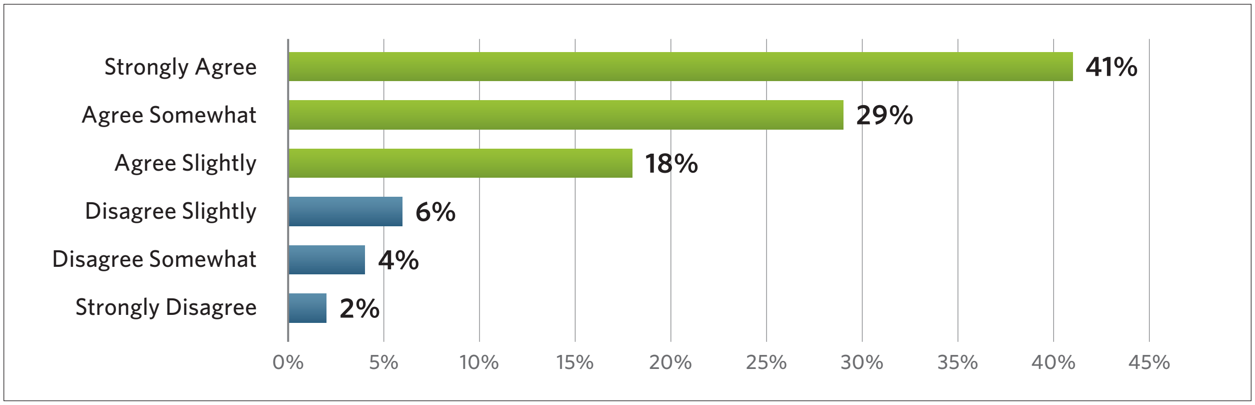
Sophisticated business models used by cybercriminals have allowed tools and services once reserved for the cybercrime elite to be made available on the black market as commodities and DIY kits. The more savvy criminals offer their goods and services to those who are starting out or are in need of setup and instructions. Whether selling off-the-shelf botnets, Trojans by the binary or Zeus recompiles, the underground is loaded with tools to allow any 'newbie' cybercriminal to launch an attack. With the rate of threats increasing exponentially, our study results show that companies that have a Web security solution in place significantly lower their rates of infection.

The major trends that are driving businesses and information technology today—mobility, social networking, BYOD and cloud computing—are also making organizations more susceptible to security attacks. More than ever, cybercriminals are taking advantage of these Web-based vulnerabilities, making the threat landscape more challenging.

The problem is pervasive

Incidents continue to represent a significant threat to corporate brands as well as individual users transacting business on the Internet, exploiting users' confidential information. In 2012, 79% of companies reported that they experienced one or more types of Web-borne attacks and nine in ten Web security administrators agree that Web browsing is a serious malware risk to their companies. Whether users are accessing the Web from within the corporate network or from remote endpoints and mobile devices, IT has a responsibility to protect them against data loss.

Web browsing is a serious malware risk



Web-based malware threat protection is the top challenge for 2013

Web security administrators surveyed ranked protecting corporate networks against Web-based malware threats as the number one security challenge and preventing data breaches the number two challenge in 2013. Web-based malware threat protection is driven largely by the growth of malware networks as a mode of attack. Despite the obvious awareness of the risks, only 56% of participants said they had implemented Web security protection.

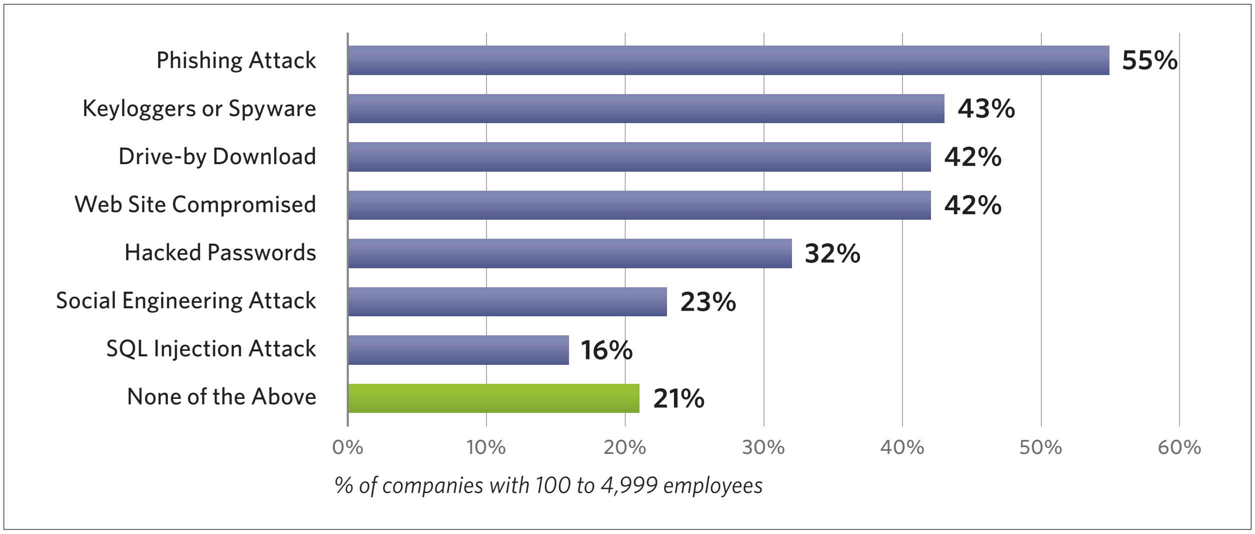
Top Web security challenges in 2013

Based on top two security challenges selected	Firms with 100 to 4,999 employees
Web-based malware threat protection	42%
Preventing data breaches	32%
Securing remote users (distributed workforce)	30%
Enforcing Internet use policies	25%
Regulatory compliance	20%
Content filtering	19%
Managing user identities and access control	18%
Guarding against zero-day attacks	13%

Phishing is the most prevalent Web-borne attack

Phishing represents one of the fastest-growing causes of breaches and data loss as cybercriminals become progressively adept at luring users into divulging sensitive corporate data. As a point of fact, more than half of companies surveyed experienced phishing attacks in 2012. Phishing is particularly challenging because cybercriminals launch new sites that masquerade as legitimate sites so quickly and for such a short period of time that most existing Web security fails to detect them.

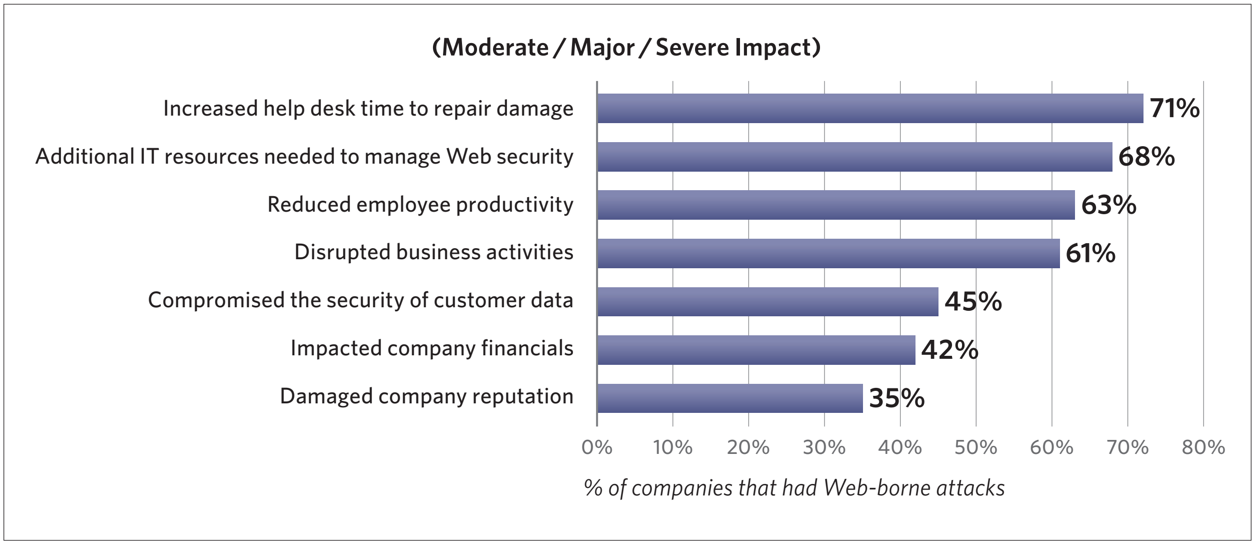
Security breaches via the Web in 2012



Web-borne attacks are disruptive

When cybercriminals attack, companies suffer direct and indirect costs in the form of increased help desk time to repair damage, additional IT resources to manage Web security, reduced employee productivity and disruption of business activities. More severely, 4 in 10 companies reported that Web-borne threats compromised the security of customer data and impacted their company's bottom line. Attacks that use spam, spear phishing and "drive-by" downloads increase the cost of data breaches. Many advanced persistent threats use these methods to gain a foothold in corporate networks.

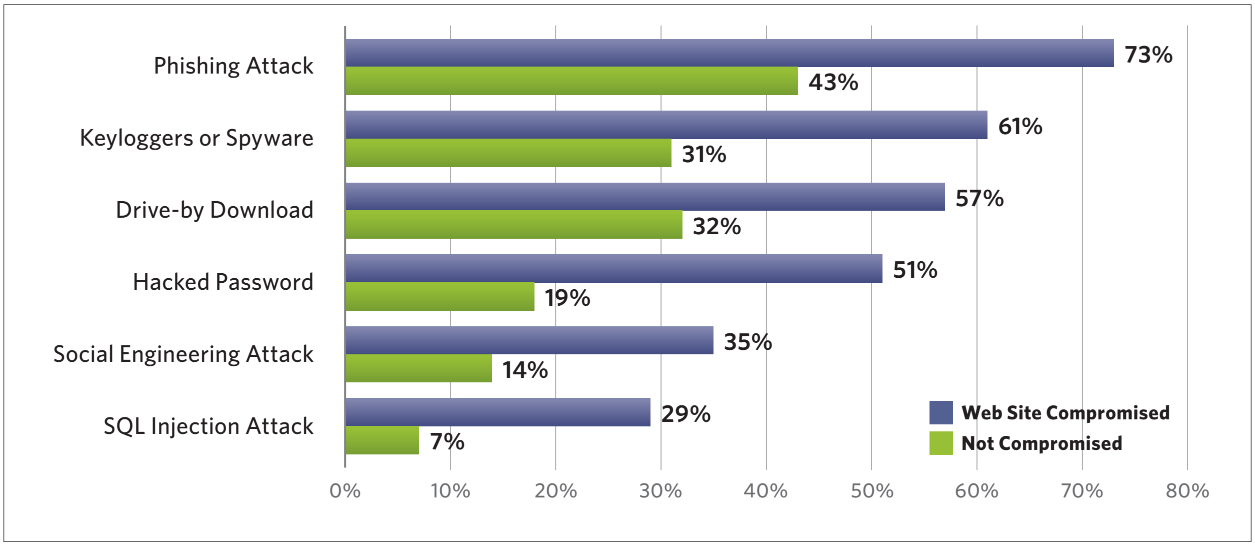
Web-borne threats a burden on companies



Consequences of Web site compromises are severe

Four out of ten companies surveyed had their Web sites compromised in 2012, which allowed cyber-criminals to hack into vulnerable sites to illicitly use a reputable domain or misappropriate resources from Web servers. Companies whose Web sites were compromised reported significantly higher rates of phishing, keyloggers/spyware, drive-by downloads, hacked passwords, social engineering attacks and SQL injection attacks. An alarming 57% of companies whose Web sites were compromised had the security of customer data breached, 55% reported a significant impact on company financials and 46% said the company's reputation was damaged.

Assaults correlated with Web sites being compromised

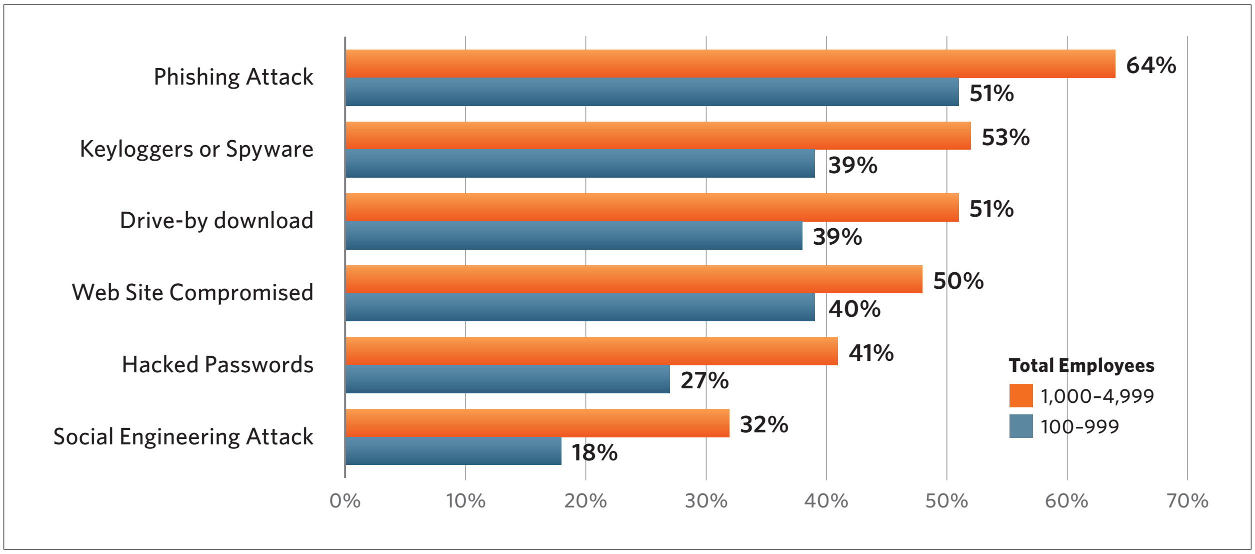


Larger companies at higher risk of data loss

Research shows that the larger organization, the greater the risk of breaches or incidents. Compared with firms that have 100 to 999 employees, companies with 1,000 to 4,999 employees are at higher risk of Web-borne attacks. The majority of large companies were victims of phishing attacks, keyloggers or spyware and drive-by downloads. Large companies also have higher rates of compromised Web sites, hacked passwords and social engineering attacks.

Web-borne attacks affect large companies more seriously. Among companies with 1,000 to 4,999 employees, 65% reported the attacks disrupted business activities, 45% said company financials were negatively impacted and 38% reported the reputation of their company was damaged.

Larger companies experience higher rates of Web-borne attacks



Web-borne attacks are costly to businesses

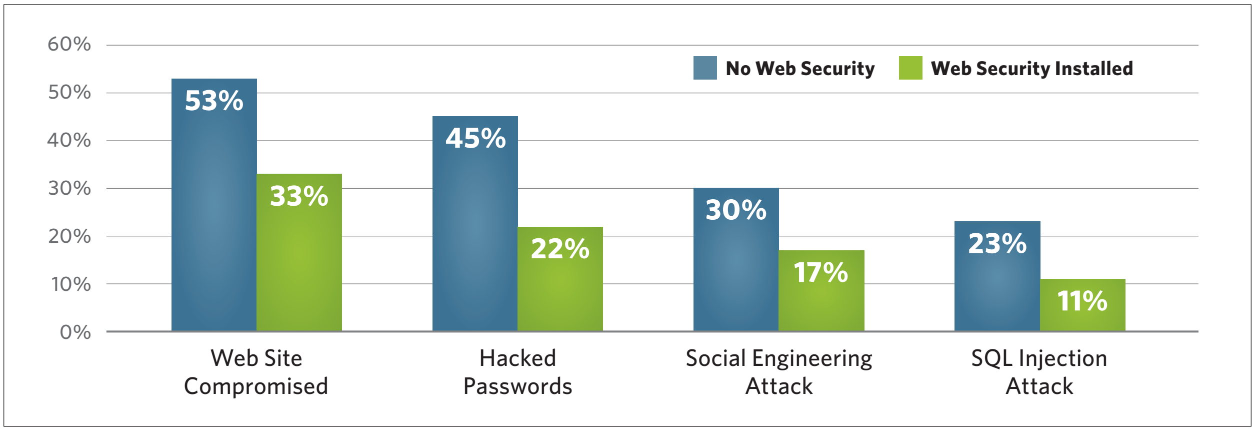
Successful malicious attacks can be devastating and costly. In the US, 15% of Web security executives estimate the cost of Web-borne attacks at $25,000 to $99,999, 13% at $100,000 to $499,999, and 6% at $500,000 to $10 million. Additionally, in the UK, 22% of Web security executives estimate the cost of Web-borne attacks at £25,000 to £99,999, 8% at £100,000 to £499,999 and 8% at £500,000 to £4 million.

44% of companies are unprotected from cybercrime.

Companies without Web security are at higher risk

Four out of ten companies have not implemented Web security and are suffering higher rates of Web site compromises and social engineering attacks. In addition, unprotected companies are twice as vulnerable to having passwords hacked and SQL injection attacks. However, 26% of companies protected by Web security had no incidents in 2012, and when a Web security solution is in place, companies also have fewer types of Web-borne infections.

Web-borne attacks lower for companies with Web security



Internet use policies in place but ineffective

While the majority of companies have an employee Internet use policy already in place, almost half of them use only the honor system or no method at all to enforce the policy. The majority of companies use network monitoring and Internet policy software. This data shows the most common non-work activities prohibited by Internet use policies and it's alarming to see companies perceive blocking social media sites more important than users shopping online.

Non-work activities prohibited by employer

Prohibited by Internet use policy	**Companies with Internet Use Policies**
Gambling online	83%
Streaming music or video	62%
Downloading media	60%
Social networking	50%
Blogging	50%
Tweeting	45%
Shopping online	44%
Instant messaging	38%
Peer-to-Peer networking	37%
Accessing personal Web mail accounts	26%
None of the above	3%

53% of companies without Web security had Web sites compromised.

What can organizations do?

Webroot advises companies to implement a secure Web gateway solution that is effective in this new environment, as well as easy to deploy, quick to respond and flexible as threats change. This outer layer should be in addition to any endpoint or mobile protection plan. Given the high mobility of today's workers a cloud-based Web security service that intercepts traffic from both within and outside the network is highly recommended.

As the survey has clearly shown, companies need to take the following steps to reduce the risks associated with this rapidly changing threat landscape.

Improve Productivity for Business Unit Management

While business unit and functional managers are interested in maintaining IT security, they also place a high value on improving worker productivity. That includes stopping workers from engaging in time-wasting activities. And today, surfing the Web is a major time wasting activity for many employees. Web security should allow them to enforce granular access rights to the Web including site, time of day and even quotas.

Educate Employees on Acceptable Use of the Internet

Employee acceptance of security measures and acceptable-use policies is a key success factor for IT security. The ability to remind employees that their Web use is monitored, policies are enforced and why they are in place encourages compliance.

Reduce Costs for CIOs and IT Managers

CIOs and IT managers not only have a responsibility to improve security, but they also have a strong interest in reducing IT costs. They can reduce network and storage costs by limiting streaming media, prohibiting very large file downloads and blocking spam. In most organizations, these are among the top bandwidth and storage hogs. Companies can also reduce their support costs by blocking malware, so that fewer computers need to be cleaned or reimaged.

Verify Compliance for Compliance Officers and Auditors

Compliance officers and auditors have the unenviable task of verifying compliance with government and industry regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, PCI DSS, HIPAA, HITECH and various European Union data protection directives. Requirements include showing that Internet acceptable-use policies are in place and being enforced and providing security measures mandated by some of the regulations.

Survey Methodology

In 2012, Webroot commissioned a study to measure the prevalence of Web-borne attacks and identify factors that mitigate the consequences. The scope of the research included companies with 100 to 4,999 employees that currently have a Web security solution or plan to implement one in 2013. From December 20 through December 24, 500 Web security decision-makers (404 in the US and 96 in the UK) completed the online survey hosted by Qualtrics. Research Now provided respondents from their online panel of IT and business executives, and Lawless Research provided quantitative data analysis. The margin of error for the study is +/- 4.4 percentage points at the 95 percent level of confidence.

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot® SecureAnywhere™ offerings for consumers and businesses. Webroot also offers security intelligence solutions to organizations focused on cyber-security, such as Palo Alto Networks, F5, Corero, SOTI, NEC, FancyFon and others. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held security organization based in the United States. For more information, visit http://www.webroot.com or call 800.772.9383. Read the Webroot Threat Blog: http://blog.webroot.com. Follow Webroot on Twitter: http://twitter.com/webroot.

Webroot Headquarters:
385 Interlocken Crescent, Suite 800, Broomfield, Colorado 80021 USA