webroot®

PUBLICATION DATE
11 February 2011

How to Protect Your Business from the Coming Malware Storm

Industry Research

Table of Contents

Introduction 3

Malware evolution follows Web evolution 3

- Broader, faster 4
- Growing financial focus 4
- Social networking 5
- Consumerization 5

The malware storm. 5

Implications for small and midsize businesses 5

- The end of perimeter security 5
- Signature-based security reaches its limits 6
- Heuristics compromise performance 6
- Management becomes unstable 6
- Advanced security will go neglected 6

Security as a service: the cloud alternative 7

- Delivers better economics 7
- Protects your business 8
- Offloads processing burdens 8
- Keeps you ahead 8

Why doesn't everyone do this? 9

Why Webroot? 9

Introduction

For the past few years, it seemed that mature on-premise antivirus, antispam, and Web defenses were making progress against the rising volume of malicious code aimed at businesses from the furthest corners of the Web. But a new generation of organized, well-funded, and financially-motivated online criminals are now launching attacks using social networks, exploiting consumer and mobile devices and vulnerabilities in Web applications, and deploying blended threats to attack financial targets and individual businesses.

These new attacks use human intelligence coupled with unique or customized code across multiple vectors to evade or overwhelm firewalls, filters, and endpoint defenses. Their sheer volume will force businesses to overspend, compromise performance of their networks and systems, or expose themselves to greater financial and regulatory risks—or find new ways to defend their operations and business information.

The malware storm will force the cost and complexity of premise-based protection to levels sustainable only by national governments and multinational corporations. To keep from being overwhelmed, small and midsize businesses must move defenses outside their own walls, to stop malicious code before it reaches their gateways, servers, and data stores. This paper describes the evolution and future of the online threat environment, and outlines the security, economy, performance, and control available to smaller businesses who act now to adopt Security as a Service.

Malware evolution follows Web evolution

Malicious code adapts to computing environments, from prank programs on mainframes, boot-sector viruses on floppy disks, and worms spread on local networks and in multitasking UNIX systems. Wide availability of broadband Internet connections led to an explosion of viruses and worms, a trend that continues today.

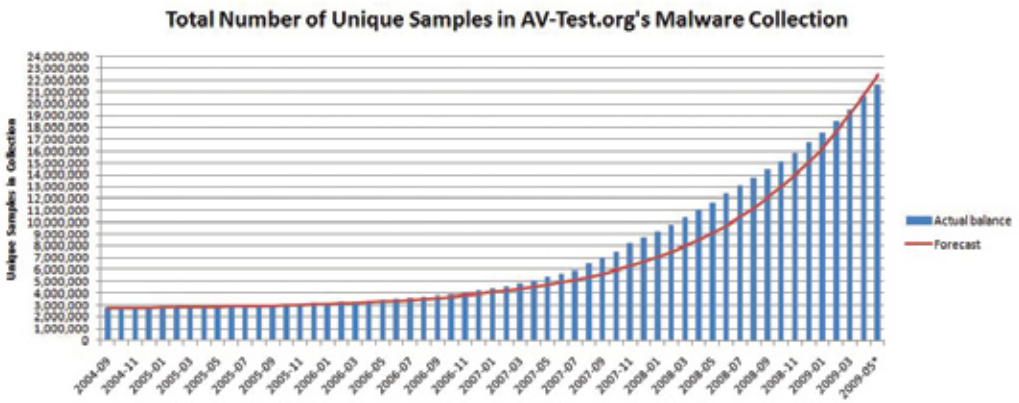

Figure 1: Wide availability of broadband Internet connections led to an explosion of malware.

The variety of malware is not necessarily a problem by itself. If the code has been identified and its signature published, network and endpoint defenses may be adequate against it until volumes become overwhelming. But new malware is appearing at an accelerating rate.

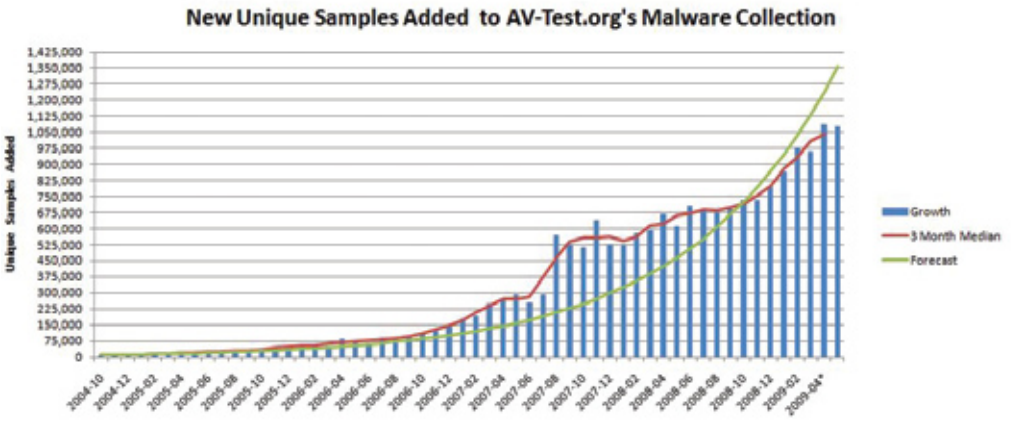

Figure 2: New malware is appearing at an accelerating rate.

The Web continues to evolve, growing broader and faster, more financially-focused, and including more Web-enabled devices and social applications. These trends all but guarantee that malicious code will grow more prevalent, harder to detect and defend against, and more dangerous.

> Financial information is sold on a **growing network** of underground exchanges.

BROADER, FASTER

The Internet connected to its five-billionth device sometime in August 2010; Cisco Systems predicts that the combination of new smart phones and other devices, increased usage, and application-driven growth will multiply global IP traffic another five times by 2013. Much of that growth is occurring in emerging markets, much of it is direct machine-to-machine communication, and not all of it is benign.

Despite much smaller national IT infrastructures, China and Brazil now rank just behind the US in overall malicious activity, a category that includes malicious code, spam zombies, phishing hosts, bots, and attacks. And stopping attacks that originate in fast-growing, low-enforcement jurisdictions is a slow, hit-or-miss process.

Of course, Web growth is more than geographic. The proliferation of high-bandwidth connections and the efficiency of browser-based applications interfaces have made Web applications productive for businesses and engaging for users. But they also open vulnerabilities for malicious code, and today, 85% of new malware uses the Web as its primary attack vector, and Web applications now account for 60% of all attacks on the Internet. A growing proportion of these are symbiotic threats, which combine multiple functions to propagate and persist, and can't easily be categorized according to their behavior.

GROWING FINANCIAL FOCUS

Financial companies are the key targets of identities exposed in hacker attacks, data breaches, and phishing exploits, and financial information is sold on a growing network of underground exchanges. The volume and liquidity of stolen financial information supports growing professionalization of cybercrime, leading to more sophisticated attacks.

But even as the sophistication of high-end malware grows, the entry threshold for cybercrime is falling. Exploit kits that compromise vulnerable machines and do-it-yourself malware kits allow relative novices to create customized password-stealing and financial data-gathering malware—and even zero-day exploits and botnets—using plug-in features of malware purchased online.

Both sophisticated attacks and malware customized from kits show up in "advanced persistent threats" (APT)—attacks aimed at a single company or even individual. Unlike global attacks that count on speed of propagation to infect as many systems as possible before detection, this new malware evades detection by staying off the grid while carrying out long-term attacks on financial targets.

SOCIAL NETWORKING

Users of social networking applications like Facebook, LinkedIn and Twitter put personal information online with little or no attempt to disguise or protect it. In most cases, sharing of personal information is the reason they participate. And while concerns about individual privacy are widely reported, the effects on businesses are less well known.

But to a criminal planning to attack a business, social applications can be an attractive first step. Social networks identify friends, interests, and employers that data aggregators can link to email and home addresses, purchasing behavior and more—all of which can be used to create a personalized "spear-phishing" appeal, or the first phase of an Advanced Persistent Threat against their employer.

Worse, as many as 30% of US employees connect with social-networking sites from work, over their employers' networks or from their personal devices—a figure that is expected to rise to 60% in three years or less [Unisys Information Worker Survey]. This may open an attack vector that starts with an innocent-looking appeal from an apparent friend or colleague which then—unless the employee is alert and well-trained—may prompt the user to install a keylogger from an email attachment, or download code from a malicious Web site.

CONSUMERIZATION

We have already seen that the growth of IP-enabled consumer devices—personal laptops, netbooks, smart phones, tablets, gaming platforms and more—is a major factor in the expansion of the Web. But these devices represent more than just additional endpoints. They operate using a variety of proprietary and open-source protocols, few of which are compatible with business-grade security and management solutions. And because they routinely operate outside business networks, they send company information and access company applications across multiple unprotected channels.

> "Traditional firewall and antivirus security offers little protection as email, CRM, storage, and even office applications move to the Web.

The malware storm

Financially-motivated criminals with highly-automated tools, operating from more connections in more places and exploiting new social and network vulnerabilities—any one of these factors elevates risk; taken together, they multiply it. Malware is becoming as easy to create and target as spam. And just as spam now constitutes 90% of all email, Webroot predicts that businesses will soon face an environment in which most of the code they encounter on the Web is malicious, much of it is unique or uncatalogued, and some of the worst examples are aimed directly at them. This environment will force dramatic changes in security strategy at all but the largest businesses.

Implications for small and midsize businesses

Multinational enterprises and national governments operate at a scale that can respond to new threats by building infrastructure and hiring specialist staff. Small and midsize businesses, on the other hand, may find that it forces them into unacceptable compromises among security, performance, and cost unless they can find new ways of doing things.

THE END OF PERIMETER SECURITY

If laptops and Wi-Fi signaled the beginning of the end for perimeter-based security, smart phones, social networking and Web applications are the end of the end. Smart phones and social networks let employees transmit business-relevant information over communications channels their employer can't control. Traditional firewall and antivirus security offers little protection as email, CRM, storage,

and even office applications move to the Web. And the rise of virtual desktops introduces a wildcard—locked-down desktop images can be more secure, but only if the endpoints themselves are secured by virtualization-aware security solutions.

SIGNATURE-BASED SECURITY REACHES ITS LIMITS

Signature-based blocking of malicious code is the mainstay of today's anti-malware solutions. But signature-based antivirus can no longer keep up with the volume of malware in today's environments. In the case of Advanced Persistent Attacks, malicious code can extract company information for months, evading detection because it has a single target. Signatures typically do not exist for injection attacks on vulnerabilities in Web applications. And even when malware signatures exist, distributing them to all the relevant servers and endpoints consumes network bandwidth and processor cycles as malware volume builds.

HEURISTICS COMPROMISE PERFORMANCE

Understanding the limits of signature-based security, most companies back it up with a layer of network-based intrusion-detection or prevention software. These technologies examine the code for suspicious processes or targets, or even execute the code in a protected "sandbox" to see what it does. Such analysis, of course, takes much more time than application of a single signature, but forms an important second line of defense.

Many antivirus software providers also build anti-malware heuristics into their solutions to stop zero-day threats. But even the best of these can only detect about 60% of zero-day malware, and they generate false positives at a significant rate.

But when the volume of unique and custom malware rises to anticipated levels, execution of heuristic protocols will become a significant deadweight loss of business productivity.

MANAGEMENT BECOMES UNSUSTAINABLE

At any scale smaller than multinational enterprises, businesses struggle with security management—economizing by combining it with the compliance function, for example, or merging it into operations. But the new malware environment demands specialized expertise, time, and dedicated resources to carry out functions like these:

- Analyzing new malware, including unique, custom, and persistent threats
- Creation and enforcement of security and acceptable-use policies for laptops and other mobile devices
- Defining and implementing context-sensitive protection for confidential information
- Keeping pace with security updates, vulnerability patches, and security software upgrades

It's more than a matter of making time—fully effective security management, even for a small firm, already strains resources. The hiring, training, management, infrastructure, software needed to address tomorrow's threats will put security management beyond the reach of most businesses.

ADVANCED SECURITY WILL GO NEGLECTED

The sections above address baseline IT security—the kind companies used to create with firewalls, boxed software, and an appliance or two. But as we've seen, criminal exploits and malware evolve continuously, and as businesses struggle to maintain effective protection today, they risk neglecting emerging disciplines like these:

Data security Malware is bad primarily because it exposes confidential data, imposing direct financial, remediation, and long-term reputational costs. But data security is bigger than malware alone. Data-loss prevention (DLP), content filtering, and encryption solutions are the next step in business security—ring-fencing the target in addition to guarding the doors.

Security best practices and policies Large enterprises dedicate entire departments to compliance with IT best practices and policy frameworks, but it's a rare midsize business that can afford even a single fulltime staffer. But policy-based, end-to-end consistently enforced best practices are a highly effective way for any business to upgrade its security posture.

Vulnerability scanning Resource constraints keep many small and midsize businesses from identifying and patching known vulnerabilities—even though most Web-based malware exploits one or more of them.

Security as a Service: the cloud alternative

The malware storm puts businesses in a corner bounded by security, performance, and cost—is there a way out? Yes there is—and fittingly, it leads right back to the Web.

> "Costs are spread over multiple clients for world-class protection **at a business-class price.**

Security as a Service, or SaaS, is a comprehensive set of security applications, delivered to clients as services through the cloud. The security provider backs its services with a global network of data centers equipped and staffed to deliver enterprise-grade security and security management. Clients keep their firewall(s) in place, and deploy lightweight endpoint security solutions to block local threats and remediate systems. They then route all Web and email traffic to a security provider's cloud-based distributed datacenter network, where traffic is scanned, cleaned and routed back to the customer over high-speed, low-latency communication links, as detailed below:

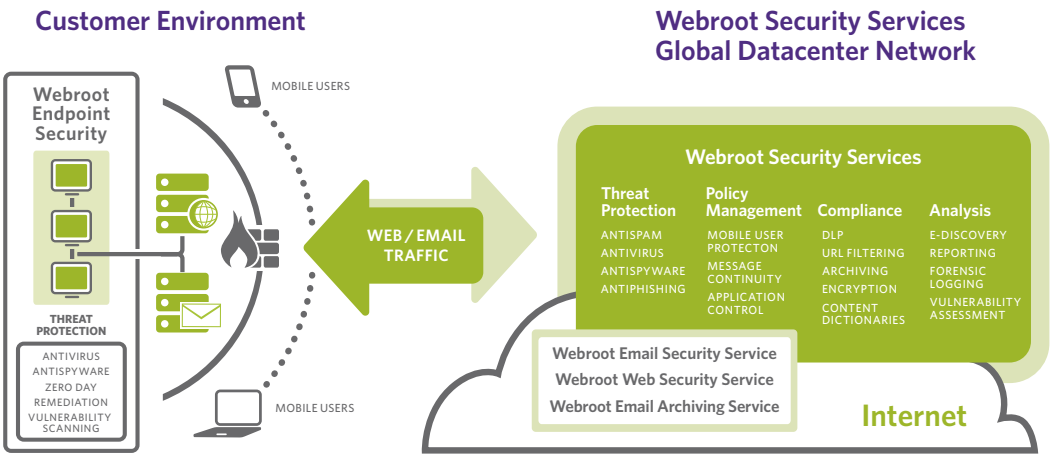

Figure 3: The Webroot Security Service Approach

DELIVERS BETTER ECONOMICS

The business value of SaaS comes from economies of scale—the ability to give many smaller clients the infrastructure, specialized skills, and service levels few companies can afford. Compared to on-premise solutions, SaaS economies include:

- Reduced burden on company IT staff and resources
- Less maintenance required
- Simplified management: less time, fewer errors
- Rapid deployment, reconfiguration, and upgrade
- No hardware or software to purchase or licenses to manage
- Consolidation of security solutions with one vendor and one support team
- Quick scalability with no capacity ceiling

But the most compelling economic rationale for SaaS is "more for less"—world-class security and security management for a price lower than most companies pay for "just good enough" protection.

PROTECTS YOUR BUSINESS

SaaS provides better protection from the malware storm than all but the most expensive on-premise solutions, and neutralizes the trends that threaten to overwhelm them:

- **Geographic and botnet threats** are addressed with research-backed global URL reputation assessment
- **Financially-focused targeted threats**—even "one-off" targeted attacks—receive in-depth heuristic analysis without tying up business resources
- **Social-networking exploits** are thwarted by correlating data across multiple security solutions: Web and email filters, for example
- **Mobile laptops and users** protected through the nearest provider data center for efficient, location-independent protection for all users

OFFLOADS PROCESSING BURDENS

Because email and Web traffic is routed through one of the service provider's data centers, the "heavy lifting" of scanning email and Web traffic, applying heuristics to suspicious code, and updating signatures and rules is all done away from clients' facilities and off client systems. This frees up processing cycles and bandwidth better and faster than expensive on premise solution upgrades, and accelerates returns on SaaS investments.

Even more offsite "heavy lifting" goes into providers' infrastructure and software management and maintenance, best practices development and implementation, compliance initiatives, staffing, research, and more—with costs spread over multiple clients for world-class protection at a business-class price.

KEEPS YOU AHEAD

With antivirus, antispam, and antispyware executed and managed in the cloud, SaaS clients remain protected and productive against malware threats, even as they tax the budgets and computing resources of businesses that try to "go it alone" using premise-based solutions.

Those same provider infrastructure and personnel resources provide advanced security solutions, including:

Data security and compliance solutions that filter, selectively encrypt, or send alerts based on the content of both inbound and outbound traffic

Compliance acceleration from fully-documented security best practices delivered as a single service package

Archiving offsite, offloading client storage, network, and processor overhead, reducing clutter and duplication, and simplifying regulatory compliance and legal discovery

Why doesn't everyone do this?

Very large companies and governments that can maintain their own global network of security-focused data centers may choose to keep security as a core competence managed in-house. But for all but these few hundred organizations, the future of security is in the cloud.

Concerns about cloud-based security, which by its nature shared across multiple clients, come down to a few questions like these:

- **Performance** If all my traffic goes through a provider's data center, won't that cut throughput and latency?
- **Reliability/Availability** How do I know my provider will stay available?
- **Vendor lock-in** Once I route all my traffic through a provider, how easy is it to reclaim, or route through a different provider?
- **Control** Will I have control over my policies and data, or need to surrender them to some "one size fits all" solution?

Answers will vary from SaaS provider to provider, but two factors are critical:

Transparency, from immediate feedback online, through alerts and status reports, to process documentation and long-term trending studies that show you what your SaaS vendor does, for an evidence-based discussion

Accountability, expressed by clear SLAs with performance guarantees, to bind your SaaS provider to promises and claims.

> "The future of security is **in the cloud.**

Why Webroot?

Webroot is a leading provider of Security-as-a-Service solutions for businesses and consumers worldwide. Webroot's powerful suite of hybrid and cloud-based solutions for businesses integrate security, data protection, data management, and policy management technologies to help organizations of all sizes improve threat management, protect confidential data, and meet industry compliance concerns. The Webroot solution provides customers with a layered approach to security including products for Web and email security, email archiving and endpoint security. Offerings can be implemented as an integrated suite or as individual point products. All Webroot products come with the industry's best customer support and are backed by strong service level agreements (SLAs) that guarantee service performance and availability.