Can Collective Cloud Intelligence Combat Today’s Financial and E-Commerce Threats?

A Webroot publication featuring research from Gartner

Issue 1

2 Welcome
3 From the Gartner Files: Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats
7 Big Data and the Webroot Intelligence Network (WIN)
8 Combating DDoS Attacks with IP Reputation
9 Preventing Fraud in the Face of Social Engineering Schemes
10 A Layered Approach: Not all Security is Created Equal
11 Summary
12 About Webroot
Welcome

Today’s cybercriminals are more organized than ever before and the impact of their crime is felt across the financial and e-commerce sectors the world over. As more and more people access financial services and accounts from personal devices, service providers and their users have become the primary targets for online scams. Year over year, newer and more inventive social-engineering techniques, such as watering hole attacks and spear phishing, are combined with malware attacks to trick people into handing over their financial and personal information, while the security industry fails to provide effective solutions to these problems — that is, until now.

Webroot SecureAnywhere products define the next generation of real-time threat identification and prevention by leveraging collective cloud-hosted intelligence to offer up-to-the-minute protection – both on the Web and across all device platforms. In combination with user-sourced data, Webroot’s cloud intelligence network effectively combats techniques used to circumvent traditional security solutions. Additionally, SecureAnywhere products include an ID Shield which neutralizes financial threats, a real-time Anti-Phishing service, and an IP Reputation service to help address distributed denial of service (DDoS) attacks.

In this document, you will learn how Webroot’s unique approach successfully addresses today’s financial and e-commerce threats. Using big data analytics and security intelligence from customers and technology partners worldwide, Webroot delivers millions of real-time threat decisions a day from our cloud to you and your users.

The cybercrime rate is on the rise. Gartner’s research\(^1\) shows that more than 50% of organized online attacks target financial and e-commerce services and their users. That research also confirms that people continue to be the weakest link in the security chain, and predicts that distributed denial of service (DDoS) and criminal social engineering scams will reach new levels of prevalence and deviousness in 2013. Faced with such a gloomy forecast, what can financial and e-commerce providers do to protect themselves from the onslaught of increasingly complex threats? How can we prevent sensitive data from being leaked or stolen? Is there a solution to combat today’s threats to these providers?

Simply put, the modern threat landscape is too vast and too dynamic for reactive, signature-based defenses to be effective. Rather than waiting for such threats to grow and morph as we struggle to analyze and address them individually, Webroot uses a vastly different approach. Leveraging big data analytics and threat intelligence from users and technology partners worldwide, Webroot delivers real-time protection from our security cloud to recognize threats before the competition sees them coming.

Source: Webroot

<table>
<thead>
<tr>
<th>Warnings</th>
<th>Gartner’s Recommendation</th>
<th>Webroot’s Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Attacks are the New Norm</td>
<td>Implementing DDoS Mitigation Techniques</td>
<td>IP Reputation Service to Protect Against DDoS</td>
</tr>
<tr>
<td>Hackers Steal Money and Account Information</td>
<td>Strengthening Risk Controls in less Secure Customer Channels</td>
<td>Identity Protection and Real-Time Anti-Phishing Services to Prevent Theft of Sensitive Data</td>
</tr>
<tr>
<td>People are the Weakest Link</td>
<td>Implementing layered fraud prevention controls</td>
<td>Feature-Rich and Compatible with Other Security Solutions for Layered Protection</td>
</tr>
<tr>
<td>Organized Gangs Responsible for at least half of the Cybercrimes Against Finance &amp; E-Comm Companies</td>
<td>Sharing intelligence to strengthen defense across enterprises</td>
<td>Big Data Analytics and Global Intelligence Cloud</td>
</tr>
</tbody>
</table>

\(^1\) Gartner, Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats, Avivah Litan, 29 January 2013
In 2013, e-commerce and financial services companies will be hit by increasingly sophisticated attackers and attacks, such as high-bandwidth DDoS attacks and devious criminal social-engineering ploys. We provide best practices so targeted firms can arm themselves and avoid costly damage.

**Impacts**

- High-bandwidth distributed denial of service (DDoS) attacks are becoming the new norm and will continue wreaking havoc on unprepared enterprises in 2013.

- Hackers use DDoS attacks to distract security staff so that they can steal sensitive information or money from accounts.

- People continue to be the weakest link in the security chain, as criminal social-engineering ploys reach new levels of deviousness in 2013.

- In 2013, organized gangs will perpetrate at least half of the cybercrimes against financial services, gaming and other e-commerce companies, as offshore gangs thrive and foreign governments look the other way.

**Recommendations**

- Implement DDoS mitigation techniques, and work with service providers to ensure enough capacity and functionality to withstand high-bandwidth DDoS attacks.

- Strengthen risk controls in traditionally less secure customer channels — notably, telephone-based channels, which are especially vulnerable during DDoS attacks.

- Implement layered fraud prevention controls that detect abnormal user and session behavior and activity, as found in the upper layers of the stack.

- Cooperate with law enforcement and industry associations, and share intelligence in a timely manner so as to coordinate a strengthened defense across enterprises.

**Analysis**

2012 witnessed a new level of sophistication in organized attacks against enterprises across the globe, and they will grow in sophistication and effectiveness in 2013.

A new class of high-bandwidth DDoS attacks of up to 70 Gbps hit top U.S. banks in the second half of 2012, justifiably causing serious concerns among bank security staff, law enforcement and bank regulators. Some banks and at least one U.S. banking regulator (the Office of the Comptroller of the Currency [OCC]) reported that fraud and customer account takeover were associated with at least some of these attacks. Beyond the banking industry, high-bandwidth DDoS attacks are becoming the new normal.

Similarly, many other examples of increasingly well-organized criminal activity across the globe have taken advantage of weaknesses in people, processes and systems. This research explores some top 2013 criminal trends and presents potential safeguards and solutions (see Figure 1).

**Impacts and Recommendations**

**High-bandwidth DDoS attacks are becoming the new norm and will continue wreaking havoc on unprepared enterprises in 2013**

A new class of damaging DDoS attacks was launched against U.S. banks in the second half of 2012. These attacks lobbed payloads of multiple megabytes that sometimes added up to about 70 Gbps of noisy network traffic blasting at the banks through their Internet pipes. Until this recent spate of attacks, most network-level DDoS attacks consumed only 5 Gbps of bandwidth. This made it impossible for bank customers and others using the same pipes to get to their websites.

Gartner expects high-bandwidth DDoS attacks to continue and to increase in frequency in 2013. Gartner also expects that at least 25% of DDoS attacks will be application-based, in which attackers send targeted commands to applications to tax CPU and memory and make the application unavailable.
Recommendations:

- Revisit your network configurations, and rearchitect them to minimize the damage that can be done. For example, consider managed DNS services, which can mitigate the impact of DDoS attacks against DNS name servers (DDoS attacks against DNS can also make websites unavailable).

- As described in “Enterprise Strategies for Mitigating Denial-of-Service Attacks,” evaluate and use ISP “clean pipe” services or DDoS “mitigation as a service” options. ISP clean-pipe services help ensure that “fill your pipe” attacks will not succeed, and most ISPs have mature service offerings that address all forms of DDoS attacks. DDoS mitigation-as-a-service options represent “middlemen” that route your inbound Internet traffic through them, detect attacks, and perform scrubbing or filtering in their Internet data centers. Some services can also mitigate DNS-focused DDoS attacks by distributing DNS name servers globally.

- Organizations that have a critical Web presence and cannot afford relatively lengthy disruptions in online service should employ a layered approach that combines multiple DOS defenses.

Hackers use DDoS attacks to distract security staff so that they can steal sensitive information or money from accounts

Gartner clients have reported instances of fraud and customer account takeover associated with the high-bandwidth DDoS attacks launched during the second half of 2012. Furthermore, on 21 December 2012, the OCC issued an alert to U.S. banks on the recent spate of DDoS attacks. The regulators acknowledged the existence of different attacker groups — some politically motivated, and others financially motivated — and confirmed that these DDoS attacks have led to or been associated with fraud and customer account takeover.

Enterprises subject to DDoS attacks should take steps in several areas outlined below to mitigate potential damage from these attacks.

Recommendations:

- Collaboration:

  - Inform law enforcement about attacks in a timely manner.

  - Cooperate with industry associations to share intelligence that can be acted on collectively and quickly. For example, work with the Financial Services Information Sharing and

---

<table>
<thead>
<tr>
<th>Impacts</th>
<th>Top Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-bandwidth denial-of-service attacks are becoming the new norm and will continue wreaking havoc on unprepared enterprises in 2013.</td>
<td>Implement DDoS mitigation techniques, and work with service providers to ensure enough capacity and functionality to withstand high-bandwidth DDoS attacks.</td>
</tr>
<tr>
<td>Hackers use DDoS attacks to distract security staff so that they can steal sensitive information or money from accounts.</td>
<td>Strengthen risk controls in traditionally less secure customer channels — notably, telephone-based channels, which are especially vulnerable during DDoS attacks.</td>
</tr>
<tr>
<td>People are still the weakest link in the security chain, as criminal social-engineering ploys reach new levels of deviousness in 2013.</td>
<td>Deploy layered fraud prevention to help stop attacks from succeeding. Use behavioral profiling and entity link analysis.</td>
</tr>
</tbody>
</table>

Source: Gartner (January 2013)
Analysis Center (FS-ISAC — if your enterprise is a financial institution), the National Cyber-Forensics & Training Alliance (NCFTA), or the U.S. Computer Emergency Readiness Team (US-CERT). These well-placed groups are instrumental in data sharing across parties affected by cyberattacks.

- Fraud prevention technology investments:
  - U.S. banks: Prepare for U.S. banking regulators to step up enforcement of FFIEC guidance on Internet banking security. This is actually a good thing because regulators often drive security spending and improvements (although it would certainly be preferable if a focus on security existed independently without regulatory pressure).

- Organizational processes:
  - Strengthen backup and incident response plans and processes, and organizational support for them. These will keep operations running smoothly and securely in other nononline channels during DDoS attacks.
  - Train customer and call center agents on how to handle increased workload and call volume during DDoS attacks as customers call in trying to get their transactions executed.
  - Train call center agents in security and in how to detect and stop social engineering by the criminals using the phone channel.
  - Proactively communicate to customers the cause of the DDoS service disruption and what nononline channels are available to them for their continuing use.

People continue to be the weakest link in the security chain, as criminal social-engineering ploys reach new levels of deviousness in 2013

In 2012, Gartner clients across the globe reported several different fraud scams that took social-engineering tactics to new heights of deviousness. These scams will continue in 2013. Examples of these include:

- In Europe, criminals showed up at people’s residences dressed as police or bank officers and told the residents therein they had detected unusual activity on their bank accounts. The imposters said they were there to help them through an account migration process to move their money from the alleged compromised account into a new one. The criminals proceeded to give the victim paperwork, which the victim duly filled out, and which in effect authorized the criminal to take over the account. This, in fact, happened, and customer funds were subsequently stolen.

- Banks also reported many instances of criminals calling out to potential bank customer victims pretending to be a bank officer, and extracting information from the victim over the phone in order to take over the account.

- In some instances, these outbound calls from the criminals to the victims took place in the middle of a man-in-the-browser attack, in which the criminal called the victim after the user read a phishing email and subsequently logged into a spoof site. In the U.K., the criminals tricked the victims into typing in money transfer confirmation codes on their smart card devices that instructed their money to be unknowingly moved into criminal accounts.

Recommendations:

- Deploy layered fraud prevention and identity-proofing techniques to help stop the social-engineering attacks from succeeding. In particular, fraud prevention systems that provide user or account behavioral profiling and entity link analysis are useful in these cases.

- Deploy call center call analytics and fraud prevention software that can help catch fraudsters calling in to commit crimes via social engineering or by using stolen identities.
• Educate customers on best security practices to help them avoid phishing attacks and social-engineering ploys. Outbound written communications or webinars can be used to educate customers.

In 2013, organized gangs will perpetrate at least half of the cybercrimes against financial services, gaming and other e-commerce companies, as offshore gangs thrive and foreign governments look the other way.

Gartner clients have reported many forms of highly organized crime across the globe — for example:

• Criminals steal user login credentials from one heist (for example, against a social network) and use these credentials to break into accounts at financial institutions, where many customers use the same credentials (login user ID and password) as they did in the system that was breached (for example, the social network). Criminals subsequently gain unauthorized access to customer accounts, funds and sensitive information.

• Organized criminal businesses established in various Asia/Pacific countries employ hundreds of hackers to attack gaming sites and engage in what is called “gold farming.” Hackers physically come to work in these offices in Asia/Pacific and launch attacks that take over customer accounts on gaming sites to steal virtual gold, currency or other rewards that players earn while playing these online games. Once the virtual goods are stolen, the hackers sell them to other players on various online forums and community sites, reaping large profits worth millions of dollars. This mainly hurts the gaming businesses that get stuck with the fraud.

• Organized gangsters are specifically targeting bank branch employees to help them with their intended crimes. They determine how best to meet these employees in social settings, such as fitness clubs or restaurants near the branch locations. The fraudsters engage in social interactions with the employees and eventually rope them into their crime schemes, usually with the promise of a lucrative financial reward for their cooperation and efforts.

Recommendations:

• Use a layered fraud prevention approach to combat crimes, as outlined in “The Five Layers of Fraud Prevention and Using Them to Beat Malware” and “The Four Layers of Identity Proofing Lead to Stronger Identity Verification.”

• Organize a security awareness program for your employees (see “Short, Focused and Just-in-Time Approaches to Security Awareness” for more information).

Evidence

1 Since September 2012, hackers have launched major disruptive DDoS attacks that temporarily took down the online banking sites of many major U.S. banks, such as Bank of America, Citi, PNC, Capital One, Fifth Third Bank, Wells Fargo, U.S. Bancorp, BB&T and HSBC. The hackers claimed to be a group called Izz ad-Din al-Qassam Cyber Fighters and preannounced the banks it was going to attack on Pastebin, another online site. The group promised in early January 2013 to continue its attacks against U.S. banks. The Obama administration says it is the work of the Iranian government.

2 On 21 December 2012, the OCC issued an alert to U.S. banks (see www.occ.treas.gov/news-issuances/alerts/2012/alert-2012-16.html) describing the DDoS attacks’ direction at national banks and federal savings associations. It reiterated that various sophisticated groups launched these attacks and that they had “different objectives for conducting these attacks ranging from garnering public attention to diverting bank resources while simultaneous online attacks were under way and intended to enable fraud or steal proprietary information.” The alert described the attacks, and gave guidance on risk mitigation and management.

3 On 17 October 2012, Prolexic Technologies, a major provider of DDoS protection services, announced that the size of DDoS attacks increased significantly against its global client base in 3Q12. In particular, during 3Q12, Prolexic mitigated seven DDoS attacks of more than 20 Gbps for its clients, when last year, this size of attack was not seen. A number of these DDoS attacks leveraged the PHP-based bot toolkit called “itsoknoproblembro” that has been used in some recent high-profile DDoS attacks against U.S. banks that reached 70 Gbps.
Big Data and the Webroot Intelligence Network (WIN)

Big data is used more and more as information technology continues migrating to the cloud. It involves the amount of information, the different types of information, and the speed at which this information is produced and distributed throughout a given sector. At more 60 million unique variants per year, the volume, variety, and velocity of malware flooding the Internet and the numerous ways in which we connect to it is staggering. Traditional antivirus vendors scramble to add new features to increase their protection levels. Unfortunately, new features need even more CPU and RAM resources, which can reduce performance and usability to unacceptable levels. The only way to keep up is to analyze huge data sets in real-time in the cloud and use this data to not only to detect, but to prevent and predict.

Big data lets us discover malware as soon as it attempts to infect a user, and then protect all other users against such attacks without the hassle of time-consuming signature updates. The Webroot Intelligence Network (WIN) integrates billions of pieces of information from multiple sources, including data from customers, test laboratories, and intelligence shared between security vendors – to create a massive malware detection net.

WIN incorporates Webroot’s patented fourth-generation threat processing and malicious code identification system, which has intimate knowledge of more than 300 million executables, including their runtime behavioral characteristics. WIN also uses systems that allow us to instantly categorize files and their interactions with other files. It uses our IP Reputation service to track every malicious IP address on the Internet and provide accurate content classification, threat reputation, and threat vector data. These systems, along with another 50+ terabytes of threat data, ensure that the Webroot Intelligence Network is always up-to-date and ready to detect new threats.

As this collective intelligence delivers comprehensive real-time protection, endpoints collect over 200 gigabytes of behavioral execution data each day. Unique URL and IP data feeds from strategic partners further enrich our malware intelligence. As a result, Webroot SecureAnywhere becomes more powerful every minute, and more effective each time an endpoint is added anywhere in the world.

Source: Webroot

FIGURE 1  Webroot SecureAnywhere System

Source: Webroot
Combating DDoS Attacks with IP Reputation

Gartner research shows that a significant portion of online attacks are perpetrated using distributed denial of service (DDoS). High-bandwidth denial-of-service attacks are becoming the new norm and will continue wreaking havoc on unprepared enterprises in 2013. Hackers use DDoS attacks to distract security staff so that they can steal sensitive information or money from accounts. The ability to quickly and accurately recognize and drop traffic from DDoS attack sources is one of the most effective prevention techniques available. Webroot’s IP Reputation service harnesses a dynamic database of over 10 million known-malicious IPs to help identify such sources.

The Webroot IP Reputation service is a constantly updated feed of currently active and malicious IP addresses. Rather than using static, rapidly out-of-date public blacklists, this service delivers dynamic IP Reputation data in near real-time (every 5 minutes) to network devices.

The IP Reputation data is gathered through a new and sophisticated sensor network specifically designed to generate security intelligence in near real-time. The sensor network identifies many key IP threats including Spam Sources, BotNets, Windows Exploits, Scanners and numerous others.

As well as providing current IP Reputation data, this service offers a major secondary benefit to integrators – it avoids the taxing security processing other IP Reputation services impose, while greatly enhancing the ability to counter IP threats.

DDoS is still a potent weapon for cybercriminals, but Webroot’s IP Reputation information stops malicious traffic at the network’s edge.

Source: Webroot
Preventing Fraud in the Face of Social Engineering Schemes

As online banking, retail, and other Web services increase in popularity, cybercrime has also become more targeted and sophisticated. Per Gartner, further attacks on financial services, gaming, and other e-commerce companies occur through social engineering schemes that steal user login credentials. In social engineering ploys, people are manipulated into giving over sensitive information for fraudulent purposes. Such scams include phishing attempts and man-in-the-middle attacks, in which users are tricked into believing they are providing credentials to a reputable entity.

Advances in technology now mean customers can access their accounts and transact from a range of devices: PCs, laptops, smartphones, and tablets. While multi-device access offers ease and convenience for the customer, it also presents increased opportunity for scam artists. Organizations now have the challenge of not only securing their customer’s PC, but also securing customers who connect from any device, anywhere. In particular, banks and e-commerce providers must respond with strong security measures to protect themselves and their customers from online attacks.

For banking and e-commerce providers, maintaining the trust and confidence of customers is critical; so providing the best possible security is paramount. Over 30 financial institutions worldwide utilize Webroot solutions to improve their online security, protect their customers, and gain access to critical security intelligence to mitigate fraud losses. Webroot products are available for numerous types of devices and offer security features such as keylogger protection, real-time anti-phishing, secure browsing, Web filtering, and password management. Our security solutions are specifically designed to address the challenges of banking and e-commerce providers everywhere, ensuring that you can transact safely no matter where you are.

Source: Webroot
A Layered Approach: Not all Security is Created Equal

Many of today’s most dangerous threats, such as advanced persistent threats (APTs), do not rely on a single method of attack. Instead, they combine several. A cybercriminal might send a phishing email to lure an employee to a website. That website could then use a “drive-by download” to infect the employee’s PC with a password-stealing trojan. A single type of protection may not be enough to stop complex attacks.

Because so much of modern malware blends several methods of attack, effective security requires a layered approach. Along with an IP Reputation service, identity protection, and an endpoint antivirus solution, Webroot’s portfolio includes a secure Web gateway to help companies protect themselves from Web-based malware, enforce Internet acceptable-use policies, and manage Web usage. Key security and management capabilities include:

- Scanning HTTP traffic and blocking malware and spyware before they reach the company network and endpoints.
- Detecting and blocking phishing attacks in real-time.
- Monitoring webpage requests and preventing users from reaching websites likely to contain malware (URL and content filtering across 80+ categories).
- Enforcing company policies by limiting access to social media, gambling, pornography, shopping, job search sites, online gaming and other non-work-related websites.
- Enforcing activity quotas that limit the amount of time individuals can spend online or the number of megabytes they can download in a day.
- Reporting Web usage, so managers can look at overall usage and patterns of visits to dangerous or time-wasting websites.

The ability to control and monitor Web usage has very important security implications. Blended attacks and APTs that count on luring employees to websites run by criminals can often be foiled by controls over Web usage. IT administrators can also use reporting to identify users who engage in risky or inappropriate behaviors on the Internet, and then educate those employees on Internet safety. Beyond security, secure Web gateways also help companies improve productivity, control bandwidth usage, and demonstrate compliance with government regulations.

Source: Webroot
Summary

Due to the variety of threats swarming the online landscape, Webroot endeavors to “close the circle” by making it easy to combine endpoint protection, mobile device protection, and Web security, all designed with a client-cloud architecture. In addition, while security vendors have, traditionally, advised against running multiple antivirus programs on the same computer, this rule does not hold true for Webroot products. Webroot’s fast, lightweight solutions run alongside those from other vendors without compromising performance or security, so you can layer your protection in the way that best suits your environment.

It is essential that financial and e-commerce services arm themselves against the assault of online threats and hacking attempts. Traditional solutions are not enough to protect institutions or their users from the complex and creative attacks launched by today’s cybercriminals. Gartner warns that DDoS attacks are becoming more and more prevalent, necessitating mitigation techniques, such as an IP Reputation service. Because cyber-attacks target financial and e-commerce companies, securing online transactions and Web surfing for both customers and employees helps prevent fraud and theft of sensitive data. As malware becomes more devious and diverse, security must be dynamic enough to protect all devices on the network perimeter.

Collective cloud security combats today’s financial and e-commerce threats through a real-time, intelligent model that doesn’t depend on signature updates, and that can be layered according to your needs. Webroot’s singular approach successfully addresses these threats using big data analytics and security data from numerous global resources to deliver instant protection wherever you and your users connect.

Source: Webroot
About Webroot

Webroot is committed to taking the misery out of Internet security for consumers and businesses worldwide. Webroot products consistently receive top review ratings by respected third parties and have been adopted by millions globally. With a wide range of online security products for home and office, Webroot protects corporate networks and allows consumers to download music, store digital files, bank, shop, surf and search – safely.

Founded in 1997, the company provides best-of-breed security solutions that protect personal information and corporate assets from online and internal threats. Based in Broomfield, Colo., the company is privately held and backed by some of the industry’s leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield. Webroot currently has approximately 400 employees worldwide.

Contact Us
Webroot
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021
USA