
Each year we publish a larger Internet Security Threat Report—this is a subset of that document which focuses on the threats that impact your website and online business. Looking back at the past calendar year it provides an insight into the state of the online world.

Online where the reputation and success of your business is often measured by the trust that your customers have in the security of your website, it is important to understand how you can maintain and build on that trust. To that end, SSL/TLS has been the key to trust on the Internet for more than a decade and will continue to be so when it comes to providing the highest levels of protection against evolving cyber security threats. And while, yes, the technology is sophisticated and leading edge, the goal is simple: to make the Internet safer to transact business—for you, your customers and everyone else with whom you interact online.

Please use this document as a reference to understand the threat landscape and understand how you can protect your company and your infrastructure.

And for more information, please call us on 866-893-6565 or visit www.symantec.com/ssl-certificates.
INTRODUCTION

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of approximately 69 million attack sensors which record thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Symantec Website Security Solutions and Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world’s most comprehensive vulnerability databases, currently consisting of more than 51,644 recorded vulnerabilities (spanning more than two decades) from over 16,687 vendors representing over 43,391 products.

Spam, phishing, and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before reaching customers’ networks. Over 3 billion email messages and more than 1.4 billion Web requests are processed each day across 14 data centres. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec’s analysts unparalleled sources of data with which to identify, analyse, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers the essential information to secure their systems effectively now and into the future.
EXECUTIVE SUMMARY

The most important trends in 2012 were:

Small Businesses Are the Path of Least Resistance for Attackers

Last year’s data made it clear that any business, no matter its size, was a potential target for attackers. This was not a fluke. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them.

This is especially bad news because based on surveys conducted by Symantec, small businesses believe they are immune to attacks targeted at them. However, money stolen from a small business is as easy to spend as money stolen from a large business. And while small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank. While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyberdefenses. Criminal activity is often driven by crimes of opportunity. With cybercrimes, that opportunity appears to be with small businesses.

Even worse, the lack of adequate security practices by small businesses threatens all of us. Attackers deterred by a large company’s defenses often choose to breach the lesser defenses of a small business that has a business relationship with the attacker’s ultimate target, using the smaller company to leapfrog into the larger one.

Additionally, small businesses and organizations can become pawns in more sophisticated attacks. Driven by attack toolkits, in 2012 the number of Web-based attacks increased by one third and many of these attacks originated from the compromised websites of small businesses. These massive attacks increase the risk of infection for all of us. But even more nefariously, as reported in our Elderwood whitepaper last year, the websites of small businesses and organizations are even being used in targeted attacks. Supplementing their phishing attacks, cyber-espionage gangs now hijack these websites, lying in wait for their targets to visit so that they can infect them. This type of attack, called a watering hole, is another way attackers leverage weak security of one entity to defeat the strong security of another.

Malware Authors Act as Big Brother

If you think someone is violating your privacy online, you are probably right. Fifty percent of mobile malware created in 2012 attempted to steal our information or track our movements. Whether they are attacking our computers, mobile phones or social networks, cybercriminals are looking to profit by spying on us. Their ultimate goal is to make money. Their method is to learn our banking information, the phone numbers and email addresses of our friends and business associates, our personal information, and even how to become us by stealing our identity.

But the most ominous example of malware authors knowing all about us is in targeted attacks. Creating successful targeted attacks requires attackers to learn about us. They will research our email addresses, our job, our professional interests, and even the conferences we attend and the websites we frequent. All of this information is compiled to launch a successful targeted attack. Once on our devices, the attacker’s tools are designed to pull as much data as possible. Undiscovered targeted attacks can collect years of our email, files and contact information.

These tools also contain the ability to log our keystrokes, view our computer screens, and turn on our computers’ microphones and cameras. Targeted attackers truly act as an Orwellian incarnation of Big Brother.

Those jobs most targeted for attack in 2012 were knowledge workers who create the intellectual property that attackers want (27 percent of all targets in 2012) and those in sales (24 percent in 2012). Interest in targeting the CEO of an organization waned in 2012; those attacks decreased by 8 percent.
EXECUTIVE SUMMARY

Zero-day Vulnerabilities Available When Attackers Need Them

Zero-day vulnerabilities continue to trend upward; 14 were reported in 2012. In the last three years much of the growth in zero-day vulnerabilities used in attacks can be attributed to two groups; the authors of Stuxnet and the Elderwood Gang. In 2010, Stuxnet was responsible for 4 of the 14 discovered zero-day vulnerabilities. The Elderwood Gang was responsible for 4 of the 14 discovered in 2012. The Elderwood Gang also used zero-day threats in 2010 and 2011, and they’ve used at least one so far in 2013.

Attackers use as many zero-day vulnerabilities as they need, not as many as they have. And Stuxnet and Elderwood make for an interesting contrast in the strategy of their use. Stuxnet remains the aberration, using multiple zero-day exploits in one attack. From what we know today, it was a single attack that was directed at a single target. Multiple zero-day exploits were used to ensure success so they would not need to attack a second time.

By contrast the Elderwood Gang has used one zero-day exploit in each attack, using it continually until that exploit becomes public. Once that occurs they move on to a new exploit. This makes it seem that the Elderwood Gang has a limitless supply of zero-day vulnerabilities and is able to move to a new exploit as soon as one is needed. It is our hope that this is not the case.

Attribution Is Never Easy

Some targeted attacks make no attempt to stay undetected. A piece of malware named Shamoon was discovered in August. Its purpose was to wipe computer hard drives of energy companies in the Middle East. A group calling itself the “Cutting Sword of Justice” claimed responsibility. Throughout 2012, DDoS attacks were launched against financial institutions. A group called Izz ad-Din al-Qassam Cyber Fighters claimed responsibility.

These attacks and others appear to be classic cases of hacktivism. However, proving attribution and motive are not easy, even when someone claims responsibility. There has been much speculation, some reportedly from the intelligence community, that the Cutting Sword of Justice and the Qassam Cyber Fighters are fronts for a nation state. Complicating what appeared to be simple hacktivism even further is the FBI’s warning to financial institutions that some DDoS attacks are actually being used as a “distraction.” These attacks are launched before or after cybercriminals engage in an unauthorized transaction, and are an attempt to avoid discovery of the fraud and prevent attempts to stop it.
2012 SECURITY TIMELINE
## 2012 SECURITY TIMELINE

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 January 2012</td>
<td><strong>Data breach:</strong> 24 million identities stolen in data breach at Zappos apparel company. <strong>Malcode:</strong> A scam involving malicious browser plug-ins for Firefox and Chrome is discovered.</td>
</tr>
<tr>
<td>02 February 2012</td>
<td><strong>Botnet:</strong> Kelihos botnet returns, four months after being taken down. <strong>Mobile:</strong> Google announces Google Bouncer, an app scanner for the Google Play market.</td>
</tr>
<tr>
<td>03 March 2012</td>
<td><strong>Botnet:</strong> Researchers take down new variant of the Kelihos botnet, which reappears in a new form later in the month. <strong>Hacks:</strong> Six individuals are arrested as alleged members of the hacking collective LulzSec. <strong>Botnet:</strong> Security researchers take down key servers for the Zeus botnet. <strong>Data breach:</strong> A payment processor for a number of well-known credit card companies, including Visa and MasterCard was compromised, exposing details of 1.5 million accounts. <strong>Mobile:</strong> A non-malware-based scam involving the Opfake gang is found that targets iPhone users.</td>
</tr>
<tr>
<td>04 April 2012</td>
<td><strong>Mac:</strong> Over 600,000 Mac computers are infected by the OSX.Flashback Trojan through an unpatched Java exploit. <strong>Mac:</strong> A second Mac Trojan is discovered, OSX.Sabpab, which also uses Java exploits to compromise a computer.</td>
</tr>
<tr>
<td>05 May 2012</td>
<td><strong>Social networking:</strong> Scammers are discovered leveraging social networks Tumblr and Pinterest. <strong>Malware:</strong> The cyber-espionage threat W32.Flamer is discovered. <strong>Certificate Authorities:</strong> Comodo, a large Certificate Authority, authenticated and issued a legitimate code-signing certificate to a fictitious organization run by cybercriminals. This was not discovered until August.</td>
</tr>
</tbody>
</table>
## 2012 SECURITY TIMELINE

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>06 June 2012</strong></td>
<td><strong>Data breach:</strong> LinkedIn suffers data breach, exposing millions of accounts.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> A Trojan by the name of Trojan.Milicenso is discovered, which causes networked printers to print large print jobs containing illegible characters.</td>
</tr>
<tr>
<td><strong>07 July 2012</strong></td>
<td><strong>Botnet:</strong> Security researchers disable the Grum botnet.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> Windows malware is discovered in Apple’s App Store, embedded in an application.</td>
</tr>
<tr>
<td></td>
<td><strong>Mac:</strong> A new Mac threat called OSX.Crisis opens a back door on compromised computers.</td>
</tr>
<tr>
<td></td>
<td><strong>Botnet:</strong> DNS servers, maintained by the FBI in order to keep computers previously infected with the DNSChanger Trojan safe, are shut off.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> A Trojan used to steal information from the Japanese government is discovered after being in operation for two years.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> A second printer-related threat called W32.Printlove, which causes large print jobs to print garbage, is discovered.</td>
</tr>
<tr>
<td><strong>08 August 2012</strong></td>
<td><strong>Hacks:</strong> Reuters news service suffers a series of hacks resulting in fake news stories posted on its website and Twitter account.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> Crisis malware is discovered targeting VMware® virtual machine images.</td>
</tr>
<tr>
<td></td>
<td><strong>Malware:</strong> W32.Gauss is discovered. The scope of the threat is concentrated in the Middle East, in a similar way to W32.Flamer.</td>
</tr>
<tr>
<td></td>
<td><strong>Certificate Authorities:</strong> Comodo incident from May discovered and details published.</td>
</tr>
</tbody>
</table>
## 2012 SECURITY TIMELINE

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
</table>
| 09 September 2012 | **Malware:** A new version of the Blackhole attack toolkit, dubbed Blackhole 2.0, is discovered.  
                **Botnet:** Security researchers disable an up-and-coming botnet known as “Nitol.”  
                **Mobile:** A vulnerability is discovered in Samsung’s version of Android™ that allows a phone to be remotely wiped.  
                **DDoS:** FBI issues warning about possible DDoS attacks against financial institutions as part of a “distraction” technique. |
| 10 October 2012 | **Malware:** A ransomware threat distributed through Skype IM is discovered.  
                **Data breach:** Customer data is stolen from Barnes & Noble payment keypads.  
                Attackers are discovered using a DDoS attack as a distraction in order to gather information that allowed them to later steal money from a targeted bank. |
| 11 November 2012 | **Hacks:** Burglars found using a known exploit in a brand of hotel locks to break into hotel rooms. |
| 12 December 2012 | **Malware:** Infostealer.Dexter Trojan horse discovered targeting point-of-sale systems.  
                **Hacks:** Attackers exploit a vulnerability in Tumblr, spreading spam throughout the social network. |
2012 IN NUMBERS
42% INCREASE
Targeted attacks in 2012

604,826
AVERAGE NUMBER OF IDENTITIES EXPOSED
Per breach in 2012

NEW VULNERABILITIES

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6,253</td>
<td>4,989</td>
<td>5,291</td>
</tr>
</tbody>
</table>

MOBILE VULNERABILITIES

<table>
<thead>
<tr>
<th></th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>163</td>
<td>315</td>
<td>415</td>
</tr>
</tbody>
</table>
ESTIMATED GLOBAL EMAIL SPAM PER DAY (IN BILLIONS)
OVERALL SPAM RATE

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Spam Rate</td>
<td>89%</td>
<td>75%</td>
<td>69%</td>
</tr>
</tbody>
</table>

% OF ALL SPAM WITH DATING & SEXUAL

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>3%</td>
<td>15%</td>
<td>55%</td>
<td></td>
</tr>
</tbody>
</table>

% OF ALL EMAIL MALWARE AS URL

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>24%</td>
<td>39%</td>
<td>23%</td>
<td></td>
</tr>
</tbody>
</table>

OVERALL EMAIL VIRUS RATE, 1 IN:

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>282</td>
<td>239</td>
<td>291</td>
<td></td>
</tr>
</tbody>
</table>

OVERALL EMAIL PHISHING RATE, 1 IN:

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>442</td>
<td>299</td>
<td>414</td>
<td></td>
</tr>
</tbody>
</table>
2012 IN NUMBERS

BOT ZOMBIES (IN MILLIONS)

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.5</td>
<td>3.1</td>
<td>3.4</td>
</tr>
</tbody>
</table>

NEW ZERO-DAY VULNERABILITIES

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14</td>
<td>8</td>
<td>14</td>
</tr>
</tbody>
</table>

WEB ATTACKS BLOCKED PER DAY

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>190,370</td>
<td>247,350</td>
</tr>
</tbody>
</table>

NEW UNIQUE MALICIOUS WEB DOMAINS

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>43,000</td>
<td>55,000</td>
<td>74,000</td>
</tr>
</tbody>
</table>

MOBILE MALWARE FAMILIES INCREASE 2011–2012

58%
TARGETED ATTACKS

HACKTIVISM

AND DATA BREACHES
Organizations with 2,501+ employees were the most targeted with 50 percent of targeted attacks destined for this size of organization, almost exactly the same percentage as in 2011. The volume of targeted attacks against organizations with 2,501+ employees doubled compared with 2011, although its overall percentage remains the same at 50 percent.

Targeted attacks destined for Small Business (1 to 250 employees) accounted for 31 percent of all attacks, compared with 18 percent in 2011, an increase of 13 percentage points. The volume of attacks against SMBs increased threefold, compared with 2011, resulting in its percentage almost doubling from 18 percent to 31 percent.
Timeline of data breaches

January saw the largest number of identities stolen in 2012, due to one breach of over 24 million identities, while the numbers for the rest of the year mostly fluctuated between one and 12 million identities stolen per month.

The average number of breaches for the first half of the year was 11, and rose to 15 in the second half of the year—a 44 percent increase.
Cyberwarfare, Cybersabotage, and Industrial Espionage

Targeted attacks have become an established part of the threat landscape and safeguarding against them has become one of the main concerns of CISOs and IT managers. Targeted attacks are commonly used for the purposes of industrial espionage to gain access to the confidential information on a compromised computer system or network. They are rare but potentially the most difficult attacks to defend against.

It is difficult to attribute an attack to a specific group or a government without sufficient evidence. The motivation and the resources of the attacker sometimes hint to the possibility that the attacker could be state sponsored, but finding clear evidence is difficult. Attacks that could be state sponsored, but appear to be rare in comparison with regular cybercrime, have often gained more notoriety. They can be among the most sophisticated and damaging of these types of threats. Governments are undoubtedly devoting more resources to defensive and offensive cyberwarfare capabilities.

Analysis

At US$194, the United States is the country with highest in cost per capita, with Denmark a close second.

In 2012, it was still unlikely that most businesses would encounter such an attack, and the greatest risk comes from the more prevalent targeted attacks that are created for the purposes of industrial espionage. Increasingly, small to medium-sized businesses (SMBs) are finding themselves on the frontline of these targeted attacks as they have fewer resources to combat the threat and a successful attack here may subsequently be used as the springboard to further attacks against a larger organization to which they may be a supplier.

Malware such as Stuxnet in 2010, Duqu in 2011, and Flamer and Disttrack in 2012 show increasing levels of sophistication and danger. For example, the malware used in the Shamoon attacks on a Saudi oil firm had the ability to wipe hard drives.²

The same techniques used by cybercriminals for industrial espionage, may also be used by states and state proxies for cyber-attacks and political espionage. Sophisticated attacks may be reverse-engineered and copied so that the same or similar techniques can be used in less discriminate attacks. A further risk is that malware developed for cybersabotage may spread beyond its intended target and infect other computers in a kind of collateral damage.

Symantec Website Security Solutions
Website Security Threat Report 2013
Advanced Persistent Threats (APT) and Targeted Attacks

Targeted attacks combine social engineering and malware to target individuals in specific companies with the objective of stealing confidential information such as trade secrets or customer data. They often use custom-written malware and sometimes exploit zero-day vulnerabilities, which makes them harder to detect and potentially more infective.

Targeted attacks use a variety of vectors as their main delivery mechanism, such as malware delivered in an email, or drive-by downloads from an infected website the intended recipient is known to frequent, a technique known as a "watering hole" attack.

APTs are often highly sophisticated and more insidious than traditional attacks, relying on highly customised intrusion techniques. While targeted attacks are growing increasingly more common, the resources required to launch an advanced persistent threat campaign means they are limited to well-funded groups attacking high-value targets.

Symantec saw a 42 percent increase in the targeted attack rate in 2012 compared with the preceding 12 months. While the manufacturing industry has become the main target accounting for 24 percent of attacks, we also saw a wide range of companies coming under attack, not only large businesses, but increasingly SMBs as well. In 2011, 18 percent of targeted attacks were aimed at companies with fewer than 250 employees, but by the end of 2012, they accounted for 31 percent.

Social Engineering and Indirect Attacks

Attackers may be targeting smaller businesses in the supply chain because they are more vulnerable, have access to important intellectual property, and offer a stepping stone into larger organizations. In addition, they are also targeted in their own right. They are more numerous than enterprises, have valuable data, and are often less well protected than larger companies. For example, an attacker may infiltrate a small supplier in order to use it as a spring board into a larger company. They might use personal information, emails, and files from an individual in such a smaller company to create a well-crafted email aimed at someone in a target company.
In 2012, we saw a big increase in attacks on people in R&D and sales roles compared to the previous year. This suggests that attackers are casting a wider net and targeting less senior positions below the executive level in order to gain access to companies. The increase in attacks has been particularly high overall in these two areas. Still, attacks in other areas, such as back-office roles, are still a significant threat.

Attackers continue to use social engineering techniques in targeted attacks. For example, messages impersonating EU officials, messages that appear to come from security agencies in the United States and target other government officials, or messages that piggyback announcements about new procurement plans from potential government clients such as the U.S. Air Force. This shows extensive research, a sophisticated understanding of the motivation of recipients, and makes it much more likely that victims will open attachments that contain malware.

**Watering Hole Attacks**

The biggest innovation in targeted attacks was the emergence of watering hole attacks. This involves compromising a legitimate website that a targeted victim might visit and using it to install malware on their computer. For example, this year we saw a line of code in a tracking script on a human rights organization’s website with the potential to compromise a computer. It exploited a new, zero-day vulnerability in Internet Explorer® to infect visitors. Our data showed that within 24 hours, people in 500 different large companies and government organizations visited the site and ran the risk of infection. The attackers in this case, known as the Elderwood Gang, used sophisticated tools and exploited zero-day vulnerabilities in their attacks, pointing to a well-resourced team backed by a large criminal organization or a nation state.8

---

**Web Injection Process Used in Watering Hole Attacks**

*Source: Symantec*

1. **Profile**
   Attacker profiles victims and the kind of websites they go to.

2. **Test**
   Attacker then tests these websites for vulnerabilities.

3. **Compromise**
   When attackers finds a website that can be compromised, they inject JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. **Wait**
   The compromised website is now “waiting” to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.
RECOMMENDATIONS

Assume You’re a Target

Small size and relative anonymity are not defenses against the most sophisticated attacks. Targeted attacks threaten small companies as well as large ones. Attackers could also use your website as a way to attack other people. If you assume you are a potential target and improve your defenses against the most serious threats, you will automatically improve your protection against other threats.

Defense in Depth

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network. Consider implementing “Always on SSL” (persistent https from logon to logoff) to encrypt data transmitted via websites. Endpoints must be secured by more than signature-based antivirus technology.

Educate Employees

Raise employees’ awareness about the risks of social engineering and counter it with staff training. Similarly, good training and procedures can reduce the risk of accidental data loss and other insider risks. Train staff about the value of data and how to protect it.

Data Loss Prevention

Prevent data loss and exfiltration with data loss protection software on your network. Use encryption to protect data in transit, whether online or via removable storage.
REFERENCES

Extended Validation SSL

For businesses with a high profile brand, using Extended Validation (EV) SSL Certificates has proven to be an effective defense against phishing scams and is one of the most effective ways to build trust online. For any online business, using SSL with EV may have a big impact on the bottom line.

Key Features of Symantec Extended Validation Certificates:

• Extended Validation triggers the green address bar in Web browsers confirming that the site has passed a comprehensive verification process
• Up to 256-bit encryption
• Norton Secured Seal with Symantec Seal-in-Search maximizes click-through and conversions
• Web-based vulnerability assessment and daily website malware scanning helps to protect your site from Web-based attacks
• Around the clock 7 day support
• Symantec SSL Assistant automatically generates CSRs and installs certificates
• Plus: SSL Installation Checker, free revoke and replace, and a $1,500,000 warranty.

Norton Secured Seal:

Turn visitors into loyal customers by displaying the seal that more online consumers recognize and trust. The Norton Secured Seal is displayed over 750 million times each day on websites in over 170 countries worldwide.

Symantec AdVantage

Symantec AdVantage monitors your site in real time it is able to spot as soon as a piece of malicious content is delivered to your site. You no longer have to wait for your traffic to suddenly fall off to find out you have been blacklisted; instead you can take action to block the network the ad appeared from and keep your customers, and your reputation safe.
ABOUT SYMANTEC

Symantec protects the world’s information and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data centre to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world.

More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

More Information

- **Symantec.cloud Global Threats**: http://www.symanteccloud.com/en/gb/globalthreats/
- **Norton Cybercrime Index**: http://us.norton.com/cybercrimeindex/
- **Symantec Website Security Solutions**: www.symantec.com/ssl-certificates