

# Web 2.0

## - The New Generation of Web Threats

---

*A ScanSafe White Paper June 2008*

TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b>	<b>2</b>
<b>1.0 INTRODUCTION</b>	<b>3</b>
<b>2.0 THE DYNAMICS OF CHANGE</b>	<b>3</b>
<b>3.0 A CHEAP FRANCHISE OPPORTUNITY</b>	<b>4</b>
<b>4.0 GOOD SITES GONE BAD</b>	<b>5</b>
<b>5.0 THE THIRD PARTY THREAT</b>	<b>8</b>
<b>6.0 THE SOCIALLY ENGINEERED THREAT</b>	<b>9</b>
<b>7.0 A BYGONE ERA</b>	<b>10</b>
<b>8.0 GETTING TO THE SOURCE</b>	<b>11</b>
<b>9.0 BLACKLISTING – PAST SUCCESS, CURRENT FAILURE</b>	<b>12</b>
<b>10.0 REAL-TIME SCANNING</b>	<b>12</b>
<b>11.0 SCANSAFE SAAS WEB SECURITY</b>	<b>13</b>
<b>12.0 SUMMARY AND CONCLUSION</b>	<b>14</b>
<b>13.0 ABOUT SCANSAFE</b>	<b>14</b>

## 1.0 INTRODUCTION

Prior to 2001, websites were relatively static, designed to push information to users in a manner that was about as interactive as leafing through a bulk mail marketing flyer. But proving that adversity can be the path to enlightenment, following the dot-com crash in late 2001 a new, stronger Web emerged. And unlike its failed predecessor, the new Web lived up to its name - sites became sticky hubs of interactive content, constantly changing and morphing based on the wants and needs of its visitors. Today, the technology that enables Web 2.0 is merely the vehicle, the transport mechanism from point A to point B. It is the user - those members of the particular Web community - who ultimately drives the destination.

Unfortunately, malicious software (malware) has also evolved. Just as technology has been replaced by users as the driving force behind websites, the computer is no longer the ultimate target of the malware. The user is the target. Today, malware possesses a single objective: to gain access to the user's private, financial, and confidential information. To gain that access, malware authors exploit the very thing that makes Web 2.0 so successful - the user's trust.

This paper addresses the complex implications and interactions of Web 2.0, the malware that exploits it, and the challenges this poses to traditional security solutions.

**“Today, malware possesses a single objective: to gain access to the user's private, financial, and confidential information.”**

## 2.0 THE DYNAMICS OF CHANGE

Modern websites bear little resemblance to their predecessors. Today's websites feature dynamically changing content delivered through a steady stream of user contributions, RSS feeds and third-party advertising. Commerce is increasingly the goal, with a large portion of active sites engaged in affiliate relationships, direct sales, or some other form of business.

Not only is the face of the Web changing, the number of websites is sharply increasing. In mid-2005 when the term Web 2.0 was first coined, there were approximately 66 million sites according to Netcraft Web Server Survey<sup>1</sup> data. As of April 2008, that number had increased 250% to 165 million. Also in 2005, Antonio Gulli of the Università di Pisa and Alessio Signorini of the University of Iowa performed a study based on search engine indexing which discovered an estimated 11.5 billion pages<sup>2</sup>. In 2008, the estimated number of Web pages is nearly 30 billion. This figure excludes archived data by the Internet Archive Wayback Machine; in 2008 the IAWM had grown to a staggering 86 billion archived pages.

Likely driven by the opportunities that Web 2.0 presents, the number of users accessing the Web has also increased dramatically. In 2005, the Internet World Statistics reported 928 million global users, approximately 14% of the total world population at the time. In 2008, the number of worldwide users had increased to 1.4 billion, or 21% of the current world population.

**“Today's websites feature dynamically changing content delivered through a steady stream of user contributions, RSS feeds and third-party advertising.”**

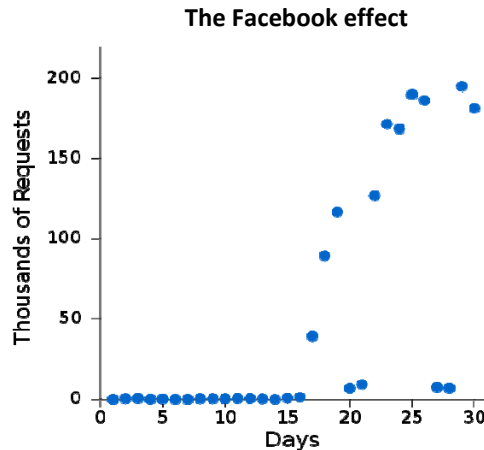
---

<sup>1</sup> [http://news.netcraft.com/archives/web\\_server\\_survey.html](http://news.netcraft.com/archives/web_server_survey.html)

<sup>2</sup> The Indexable Web, <http://www.cs.uiowa.edu/~asignori/web-size/>

## WEB 2.0 – THE NEXT GENERATION OF WEB THREATS

As with any mass-produced merchandise, quantity often comes at the price of quality. As the demand for websites increases, new and inexperienced developers flood the market to meet that demand.



Blogging and social networking comprise the largest segment of growth, a phenomenon also driven by widespread adoption of Web 2.0 technologies. The combined impact of all these factors leads to a situation in which:

- The number of websites is increasing;
- The amount of third-party content on those sites is increasing;
- The reliance on active scripting is increasing;
- Social interaction and user-supplied content is increasing; and
- The number of inexperienced Web developers is increasing.

Compounding all of these challenges, the metaphorical ‘nail in the coffin’, is a more insidious increase – the dramatic rise in both the quantity and sophistication of new malware exploiting the Web 2.0 phenomenon. This disturbing increase is coupled with a new motive: targeting the user for financial gain.

### 3.0 A CHEAP FRANCHISE OPPORTUNITY

**“The data stealing Pinch Trojan sells for as low as \$30 and the seller provides technical support.”**

Within the software industry, there exists research and development, quality assurance testing, sales, marketing, customer service and support. With money as the motive, today’s malware authors maintain a similar infrastructure. Toolkits that detect and exploit vulnerabilities on Web servers are widely available. Trojans sell openly on Internet back channels, and spam services are equally inexpensive and accessible.

Speaking at the 15<sup>th</sup> annual Defcon conference, Dr. Thomas J. Holt, computer criminologist and professor at the University of North Carolina, dissected the malware market<sup>3</sup>. According to Holt, the data stealing Pinch Trojan sells for as low as \$30 and the seller provides technical support. The package includes the buyer’s choice of packer and is guaranteed to be undetectable by

<sup>3</sup> The Market for Malware, Dr. Thomas J. Holt, presented at Defcon XV

signature based scanners at the time of purchase. For an additional \$5, buyers can get custom revisions. A \$100 server statistics software package is also available, allowing the buyer to track the infections in the same manner that a legitimate company might track sales.

Despite the similarities, there is one distinct difference between the malware market and a legitimate enterprise. With a legitimate enterprise, there is typically a trackable source of accountability. In the malware enterprise, the criminal actions are spread over a disparate, unconnected, and anonymous tier of players.

For example, an attacker purchasing a password stealing Trojan may then contract with someone else for the use of an exploit tool such as MPack, purchase a list of stolen instant messaging (IM) or email addresses from a different source, and lease time on a spam proxy from yet another source.

This business side of malware introduces many new challenges:

- Attackers don't need coding skills, they simply need a relatively small amount of cash;
- Malware of all types is readily available;
- Buyers can expect fully tested malware and technical support;
- The malware industry doesn't have an organizational hierarchy or trackable source of accountability;
- The number of new malware increased four-fold from 2005 to 2007 and is projected to increase ten-fold in 2008<sup>4</sup>.

Ironically, it is Web 2.0 – the technology that saved the Web from the dot.com bust – that facilitates the interaction, commerce, and trading that takes place among criminal coders today. And just as the attackers are using Web 2.0 technologies to facilitate the buying and selling of malware, they are also exploiting Web 2.0 technologies to foist that malware onto its victims.

**“The number of new malware increased four-fold from 2005 to 2007 and is projected to increase ten-fold in 2008.”**

#### 4.0 GOOD SITES GONE BAD

In the early stages of Web-based malware, attackers enticed visitors to infected sites via spam and other social engineering campaigns. However, as wide adoption of Web 2.0 technologies increased, many of those technologies included either exploitable vulnerabilities or were implemented in an insecure manner ripe for compromise. To increase their return on investment, attackers began exploiting these weak points, compromising legitimate and often highly trafficked sites and outfitting them with malicious, hidden iframes that automatically load the malicious code from the attacker's domain.

In and of itself, an iframe is a standard part of HTML, the language upon which Web pages are built. The iframe allows a Web developer to embed information from a source other than the page the visitor is viewing. Via the iframe tag, the developer specifies the source URL and the display size the data contained at that source will consume on the target page.

---

<sup>4</sup> <http://www.kaspersky.com/news?id=207575629>

The malicious iframe is generally configured to display 5 pixels or less of display space. As a result, the remote page is displayed in what is commonly referred to as an 'invisible iframe' – a display area so small as to be imperceptible. Only through a careful examination of the source code can the invisible iframe's presence be discerned.

**“By compromising legitimate sites to deliver malware, attackers are able to reach a much larger victim base with relatively little effort or cost.”**

By compromising legitimate sites to deliver malware, attackers are able to reach a much larger victim base with relatively little effort or cost. This has in turn led to the creation of tools and frameworks designed to deliver a turnkey solution to would-be attackers; a system that discovers and compromises susceptible sites, then delivers the exploits and malware to systems that visit those sites. Subsequently, a monetary market developed for newly discovered vulnerabilities and, in some cases, deterred traditional disclosure.

Perhaps the best known of the exploit frameworks, MPack employs malicious iframes that silently pull a remotely located file named index.php. The browser reacts to it just as it would any other index file from a legitimate website – it opens it. However, the tiny frame size makes this action imperceptible to the user. MPack's index.php then collects data about the visiting system which it sends back to the MPack server. Based on those results, the MPack framework will deliver an exploit specific to software running on the user's system at the time of attack. MPack also includes the ability to target specific countries. As such, MPack is a highly personalized attack mechanism.

MPack itself was first spotted (by PandaLabs) in December 2006, offered for license on a Russian forum. New and improved versions quickly followed and subsequently its adoption increased. This contributed heavily to a 26% increase in Web-based malware in April 2007 followed by a 36 percent increase in May 2007.

**“Today, over a dozen exploit frameworks are available, often for no or very little cost.”**

Today, over a dozen exploit frameworks are available, often for no or very little cost. Some, such as Neosploit, use layers of obfuscated JavaScript in an attempt to mask the iframe target and exploits used to deliver the malware. The Neosploit framework, which retails for \$1500-\$3000 was employed in the November 2007 compromise of Monster.com and later bundled for resell with thousands of stolen FTP credentials. The IcePack exploit framework originally retailed for \$400, but today the source code can be downloaded for free.

### **Case Study: SQL Injection Attacks**

*The Structured Query Language (SQL) is used to access information contained within a database. In some cases, the Web application may allow for the dynamic construction of queries based on user-supplied data. If the programmer has not properly managed the handling of user supplied queries, a code injection (and assorted other attacks) may be possible.*

*From October to November 2007, ScanSafe Security Threat Alert Team ('STAT') observed a SQL injection attack which resulted in malicious iframes launching exploit code hosted on [http://www.yl18.net/\\*.htm](http://www.yl18.net/*.htm). The attack was rendered using hex-encoded queries, as seen in the following abbreviated sample:*

```
DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x6400650063006C00610072
006500200040006D00200076006100720063006800610072002800380030003000300029003B007300
65
007400200040006D003D00270027003B00730065006C00650063007400200040006D003D0040006D00
2B
0027007500700064006100740065005B0027002B0061002E006E0061006D0065002B0027005D007300
65
0074005B0027002B0062002E006E0061006D0065002B0027005D003D0072007400720069006D002800
63
006F006E007600650072007400280076006100720063006800610072002C0027002B0062002E006E00
61
```

*The attack targeted the combination of Active Server Pages (ASP) and Microsoft SQL Server. The CAST command seen in the example above converts the hex into a standard string. The result is a SQL query that searches for table objects which contain text strings, looping through those found and appending the malicious iframe to each.*

*A second attack, using a near identical technique, occurred in late December 2007, extending into January 2008. The Ikea website was the first victim site observed during this busy holiday season. Other high profile sites affected included the United Nations, City of Cleveland, and State of Virginia.*

*While the number of infected sites was large (~ 50,000), with the exception of Ikea, the uc8010 SQL injection attacks typically impacted obscure pages that were not widely accessed by users. It was, however, more successful than the previous yl18 SQL injection attack, signaling that some improvements were being made to the attack methodology. And as with the previous attack, the target was the combination of ASP and Microsoft SQL Server.*

*In early April 2008, the attackers further honed the SQL injection tool to bypass Chinese government websites, to focus on English language pages, and to better target pages that enjoyed high rankings in search engines. These improvements resulted in a dramatic increase in the success of the attacks, heavily contributing to a 35% increase in ScanSafe malware blocks for the month.*

*In concert with the SQL injection attacks, a compromise of middle-tier websites was launched in late 2007. Attackers used stolen FTP credentials to outfit the sites with hidden, malicious iframes which lead to exploit and installation of password stealers and backdoor Trojans. In turn, the malware harvests additional FTP credentials, thus seeding the attack and enabling the compromise of exponentially larger numbers of sites. In April 2008, one in two ScanSafe customers attempted to access sites that had been compromised via the stolen credentials. While these customers were protected by the ScanSafe service, the numbers indicate a potential epidemic in Web-based malware attacks.*

### 5.0 THE THIRD PARTY THREAT

It's an interesting conundrum – that which makes Web 2.0 so compelling and successful, also serves as its Achilles' heel. The interconnectivity and interactive nature of today's Web creates an environment in which third-party content is not only commonplace, it's the norm. As such, Webmasters need not only be concerned with their own content and security, but also the content and security of each of their third-party content providers. And even after a site has ceased to be active, it can – through third-party content and pre-established trust relationships – do harm.

#### **Case Study – Parked Websites**

*In August 2007, ScanSafe detected malicious code originating from an advertising server hosted on an anonymous IP address allocated to a German ISP. The malicious advertisements were predominantly appearing on “parked” sites—sites that have become inactive and then used to host advertisements using a service from NameDrive. In the course of investigation, ScanSafe detected infected advertisements on 126 parked sites, one of which was the previously active georgehotelcley.com website. Links to the hotel site were found on other websites, including The Daily Telegraph newspaper. Users who clicked through legacy links on other legitimate sites were thus exposed to the risk of compromise, even though the domain itself was defunct.*

**“Malicious third-party advertising content can also impact fully functioning legitimate sites.”**

Malicious third-party advertising content can also impact fully functioning legitimate sites. Throughout much of August and a portion of September 2007, third-party advertisements infected with a downloader Trojan impacted many active, high profile sites, including TheSun.co.uk, MySpace.com, Bebo.com, PhotoBucket.com and UltimateGuitar.com.

During the course of the malicious advertising run, ScanSafe estimates that up to 12 million advertisements may have been delivered, exposing a large number of users to the Trojan. Furthermore, research has shown as much as 30 percent of vulnerable operating systems are insufficiently patched, leaving many of the exposed users open to infection.

In other cases, advertising may not be the medium, but rather the goal of the malware. In October 2007, ScanSafe investigated blocks originating with peoplesrepublicofcork.com, a site which ScanSafe believes to have been victim of compromise. ScanSafe first detected an obfuscated, invisible iframe that redirected content from several other sites, eventually leading to exploit scripts designed to install a downloader Trojan on unpatched systems. But during the course of that investigation, the content appended to the compromised site subsequently changed and began harboring hidden links and keywords in a tactic known as spamdexing. Generally, the goal of spamdexing is to increase the linked site's ranking in search engines when the associated keywords are searched upon.

Working through the layers of invisible iframes and linked sites, ScanSafe uncovered a multi-tiered rogue affiliate network that appeared to be boosting rankings for certain sites while simultaneously delivering malware via exploit. Three generic downloader Trojans, a password-stealing Trojan commonly referred to as Pakes, and a new variant of the Zhelatin family of Trojans (also known as the Storm worm) were uncovered in the course of the investigation. The

presence of a new variant of Zhelatin was particularly interesting, given that the family is considered to have amassed one of the largest botnet populations and is heavily implicated in spam and potential Distributed Denial of Service (DDoS) attacks.

Of course, not all attacks detected by ScanSafe sensors are as complex. Transparent GIF overlays are one example of a low-tech means of malware distribution. In cases such as this, the site hosting the GIF is generally not a compromised site, but rather a site that has been deliberately created and outfitted with the intent of spreading malware.

## 6.0 THE SOCIALLY ENGINEERED THREAT

Web 2.0 has fostered community and interaction across all peoples of all nations, bound together through a common interest, pursuit, or need. The resulting community-based websites result in tangible friendships with virtual strangers. Contrary to our mother's advice, talking to strangers isn't what will get us in trouble. In the Web 2.0 world, things are significantly more complicated than that.

In October 2005, a nineteen year old coder using the name Samy set out to become popular on MySpace. Samy's worm used AJAX, cross site scripting (XSS), obfuscated JavaScript and what he gently referred to as 'browser leniency' to infect every user's profile who visited his page. Subsequent visits to the profiles of those infected would also result in new friends for Samy. Within five hours, Samy gained 1,005,831 new friends, all of whom had "but most of all, samy is my hero." appended to their MySpace page.

In retrospect, the Samy worm served as a wake-up call, fully exemplifying the connectivity potential of social networking sites. All it took to infect over one million users in five hours was a single person in Samy's legitimate social circle to innocently pay a visit to Samy's profile page. The Samy worm was, for all intents and purposes, the first highly successful Web 2.0 compromise. Samy also served as a harbinger of the very real threats that were looming on the horizon.

The MeSpam Trojan is perhaps a more personal example of malware which employs social engineering. MeSpam retrieves messages and links from a remote server, and appends that information to forum posts, blog comments, and Web mail correspondence from the infected user. The link, updatable via the master server, can be changed at will by the attacker, as can the actual text used in the message.

MeSpam can also embed its message in IM chat. Other instant messaging worms may do the same, or may modify the user's away message to include a link to the worm. Unlike email, IM contacts are closed lists. As a result, a recipient of an IM chat message stands a greater chance of believing the message is legitimate and thus be tricked into visiting a malicious site and downloading malware onto their PC.

Sometimes, however, it's not malware but our own behavior that puts us at greater risk. Social networking and other Web 2.0 community sites promote a feeling of trust between the respective members. Fraudsters often attempt to become linked with other members, after which they have access to user profiles which can be used to target spam and other nefarious

**"The Samy worm was, for all intents and purposes, the first highly successful Web 2.0 compromise. Samy also served as a harbinger of the very real threats that were looming on the horizon."**

**"Fraudsters often attempt to become linked with other members, after which they have access to user profiles which can be used to target spam and other nefarious email."**

email. When even a single participant in a community is less than honorable, the other members of that same community are now at heightened risk of compromise.

Certainly, malware has always relied upon the user in order to spread. Even in the earliest days, the first boot sector viruses relied on the user to boot the computer with a floppy disk in the drive and then share that floppy disk with others. (Today, we see a similar pattern emerging with removable USB/thumb drives.) Macro viruses relied on the sharing of Microsoft Office files and were facilitated by the fact that most users of Microsoft Office at that time were on corporate networks. But it wasn't until the mass mailing e-mail worm that social engineering as a specific infection strategy emerged. Yet even e-mail worms, when contrasted to the threats today, pale in comparison.

### 7.0 A BYGONE ERA

While no malicious software can be considered benign, the change in target from computer to user does lead way to a far more insidious type of threat. Consider the CIH virus that rampaged systems worldwide in 1998. CIH delivered a damaging payload that some experts argued could be classified as hardware damage. Whether the resulting damage was due to hardware or software failure, the end result often meant an expensive repair bill for the victims.

Today's malware is much more personal and the costs much harder to recoup. A password stealing trojan can capture bank login credentials, credit card details and other sensitive financial and personal details. At stake is not the cost of a hard drive, but rather the expense of stolen funds, a damaged credit rating, outright identity theft, or all of these occurrences. International economies are also at risk. As credit card and bank fraud increases, these costs are passed on to consumers.

The enterprise has an even higher stake – all of the aforementioned risks to their employees, rising costs, and the grave risk these Trojans pose to confidential and proprietary data. Through Web 2.0, criminals can quickly and easily investigate potential targets using search engines, online telephone directories, and other web-based services. When enough information has been obtained, a highly personalized message – usually an email – is sent to the target. That email typically addresses the target by name, often includes details of a current project, and may even mention family members or include other private personal information in a bid to win the recipients trust.

The goal is to entice the recipient into believing the correspondence is legitimate and thus avoid suspicion and increase the likelihood the recipient will open the email attachment or follow a link provided in the email. The opened file typically contains a zero-day exploit. In some cases, the exploit used may be based on prior knowledge gained of the victim's computer. The exploit silently downloads and installs a data theft Trojan, usually in conjunction with a rootkit to mask its presence.

Targeted attacks can be costly both in terms of the loss of proprietary data and the loss of stockholder and customer confidence should the loss become public.

Yesterday's malware was sometimes intent on harming the computer, sometimes intent on making a public statement, and always intent on spread. It was, in many respects, the digital

**“Today's malware is much more personal and the costs much harder to recoup.”**

**“The enterprise has an even higher stake.”**

**“Targeted attacks can be costly both in terms of the loss of proprietary data and the loss of stockholder and customer confidence should the loss become public.”**

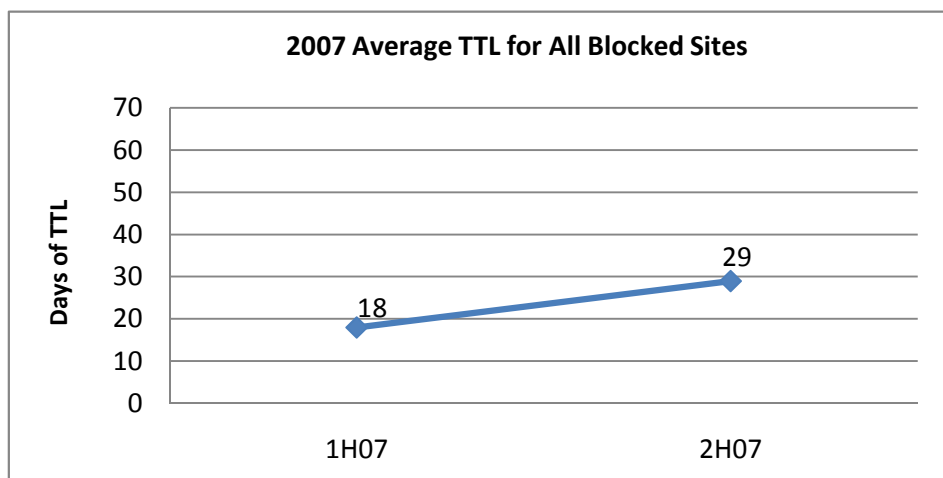
graffiti of technology. Modern day malware distributors have replaced last generation's ego gratification with monetary profit goals. Complex affiliate relationships in this black market economy dictate that infections must be controlled. Massive propagation simply arouses suspicion and forces the distributor to move on to other targets. Today's malware is much more stealthy.

## 8.0 GETTING TO THE SOURCE

There's no question that Web 2.0 has been a positive evolution for the Internet. But with its many advantages also comes a dramatically increased risk of malware exposure. Legitimate web sites which rely on Web 2.0 technologies are being compromised in record numbers, and the communities that Web 2.0 enables are being tainted by scam artists. And unfortunately, these Web threats are not only occurring more frequently, there are also lasting longer.

As discussed in ScanSafe's 2007 Global Threat Report, the number of malicious Web events increased 61% from 1H07 to 2H07 and the amount of time a malicious website remained live increased 62% from 1H07 to 2H07. In the case of zero-day events, threats for which antivirus signatures have not yet been developed, the site persistence increased from 21 days in 1H07 to 61 days in 2H07.

**"In the case of zero-day events, the site persistence increased from 21 days in 1H07 to 61 days in 2H07."**



This increased persistence is the result of many factors. Both the owner and the host of the malware delivery site may be located in geographic regions outside the confines of legal jurisdiction. In addition, the legitimate sites compromised in the attacks may be under the ownership of inexperienced Web developers who through ignorance, fear, or simply neglect, fail to react when notified.

But even when all pieces fall into place, as soon as one site is shut down, more spring up to take its place. The rising botnet populations – large collections of infected computers under the control of attackers – are often used to facilitate the attacks, thus ensuring a ready supply of compromised sites.

In many cases, the source of the compromise is somewhat outside of the Web site owner's control. Much of the dynamic content delivered on today's interactive websites comes from third-party providers. In those cases, even the most experienced Web developer may not be able

## WEB 2.0 – THE NEXT GENERATION OF WEB THREATS

to ensure security from A to Z. Furthermore, the more software and services required, the greater the exposure to un-patched and newly discovered vulnerabilities.

The increased popularity of Web 2.0 introduces new challenges:

- Jurisdictions may impede timely shutdown of rogue websites;
- Inexperienced website owners may fail to react even when notified;
- Sites that are shut down are quickly replaced by new ones;
- Site owners typically have little control over all the content on their sites;
- Sites are more complex and thus more vulnerable to exploit.

These challenges exacerbate the severity of today's malware, making it more difficult for both traditional security firms and law enforcement to counteract.

### 9.0 BLACKLISTING – PAST SUCCESS, CURRENT FAILURE

The equivalent of the virtual bouncer, blacklisting is done by compiling lists of known “bad” URLs and blocking access to the included sites. Originally compiled by collecting reports of known bad sites, blacklists today are generally created by a process known as ‘crawling’ or ‘mining’. This consists of scouring through lists of URLs, following links, scanning sites and blacklisting any sites found to be harboring malicious code.

Blacklisting, while moderately useful as adjunct protection for policy management, is less effective in the current Web 2.0 environment. The chief drawback, of course, is that content on websites is constantly changing. A scan for malware even five minutes in the past is no indication of the status of the site at the time of access. Furthermore, blacklisting can block a legitimate site that was temporarily compromised, subsequently cleaned, and no longer poses any risk to users. As such, blacklisting can be too reactive with previously compromised sites, and not reactive enough to new sites that are compromised.

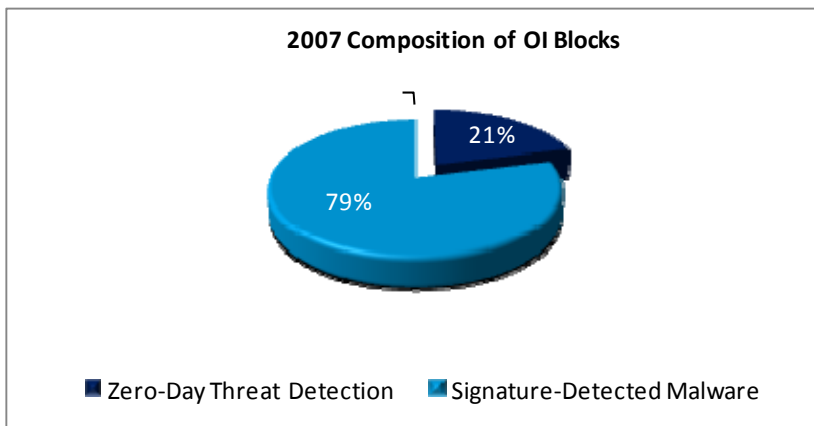
Additionally, the large amount of time required to crawl the Web means that only a small fraction of pages can be crawled. If even 450 million pages are crawled, that represents only 1.5% of the total 30 billion pages on the Web. In any event, past performance may not be indicative of future behavior – the user remains unprotected against whatever occurred between the last crawl and their current visit.

### 10.0 REAL-TIME SCANNING

To fully protect against today's constantly changing threat landscape requires a security solution that is equally dynamic. Pages must be scanned in real-time, at the moment of access. Real-time scanning ensures that all content resulting from a URL is scanned immediately, every time that it is requested. This is an important distinction from URL filtering which is based on past behavior and the assumption the malware has been previously seen. On average, 21% of the malware threats stopped in 2007 by ScanSafe OI were zero-day attacks for which signatures were not yet available – in other words, malware that had not been previously seen.

**“Blacklisting, while moderately useful as adjunct protection for policy management, is less effective in the current Web 2.0 environment.”**

**“Real-time scanning ensures that all content resulting from a URL is scanned immediately, every time that it is requested.”**



To be most effective, real-time scanning should be powered by a combination of multiple detection technologies. Used on their own, as is the approach taken by many security vendors, these technologies can often fall short. However, when these techniques are combined in a cocktail approach, their strengths are leveraged and their individual shortcomings mitigated.

## 11.0 SCANSAFE SAAS WEB SECURITY

ScanSafe is the pioneer and global leader in the provision of Software-as-a-Service ('SaaS') Web Security. ScanSafe's award winning service protects organizations of all sizes from Web based malware attacks and enables safe, productive use of the Web without incurring up-front capital, hardware or management costs.

ScanSafe SaaS Web Security is built on Outbreak Intelligence™ (OI), a proprietary security platform that detects new and known malware threats. OI scans inbound and outbound Web traffic in real-time at the moment of access, using multiple layers of zero-day threat detection combined with signature-based anti-malware scanners.

Uniquely positioned in the cloud, OI has unmatched visibility, analyzing several terabytes of Web code each day and compiling the industry's most comprehensive data set that dates back to 2004.

A URL reputation engine examines multiple parameters such as IP address information, country of the web server, history and age of the URL, and other criteria to assess the reputation of the site.

OI's traffic behavior engine analyzes network traffic patterns to identify suspicious, atypical traffic suggestive of malicious code. A code behavior engine determines the behavior of the code by modeling program logic, behavioral rules, and contextual parameters that taken together would suggest good or bad intentions.

The OI code reputation engine compares information such as type of code, history and age of the code, frequency of the code, file structure/header/content patterns, and program logic patterns to code that is known to be good or bad.

**“ScanSafe SaaS Web Security is built on Outbreak Intelligence™ (OI), a proprietary security platform that detects new and known malware threats.”**

## WEB 2.0 – THE NEXT GENERATION OF WEB THREATS

The multiple detection engines give their assessments of the code, and these assessments are then combined to produce a comprehensive view of whether or not the new code is malicious.

Customers of ScanSafe receive a 360° view of the current Web threat environment compared to the very limited view given by those utilizing URL filtering alone. This is the difference between seeing the full picture and just one piece of the puzzle. This 360° degree view of Web threats that ScanSafe delivers allows the various, traditionally disparate, components of Web security to be connected.

Real-time scanning can provide critical information on the source of malware infection and deliver immediate protection. ScanSafe allows their customers to harness the considerable benefits made available by the Web 2.0 world, without becoming one of its many casualties.

### 12.0 SUMMARY AND CONCLUSION

- As well as vastly increasing the number of URLs in existence, Web 2.0 has increased the amount of third-party content, active scripting, user-supplied content and the number of inexperienced Web developers
- Criminals are using Web 2.0 technologies to facilitate the malware marketplace and exploiting the same technology to deliver malware to its victims
- Malware's transition in target from computer to user has raised the stakes for individuals and organizations
- Over a dozen exploit frameworks are available for little or no cost, creating a turnkey franchise opportunity for would-be attackers
- SQL injection attacks are increasing in sophistication and number
- The feelings of trust and community prompted by Web 2.0 websites have made it easier for criminals to transmit malware and turn members into unwilling accomplices in attacks against members of the same community
- Shutting down the source of malware attacks is getting progressively more difficult for a number of reasons – these exacerbate the severity of contemporary malware making it more difficult for traditional security providers and law enforcers to combat
- Traditional URL filtering is not effective at enforcing security in the Web 2.0 world
- Real-time scanning of all Web traffic is the only way to harness the benefits of Web 2.0 without becoming one of its many casualties

### 13.0 ABOUT SCANSAFE

ScanSafe is the largest global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

With offices in London and San Francisco, California, ScanSafe is privately owned and financed by Benchmark Capital and Scale Venture Partners. The company received the CNET UK Business and Technology award for Security Product of the Year 2008, a 2007 CODiE award for Best Software as a Service Solution, the 2008 and 2007 SC Magazine Europe Award for Best Content Security Solution and was named one of Red Herring's Top 100 Technology companies. For more information, visit [www.scansafe.com](http://www.scansafe.com).

## WEB 2.0 – THE NEXT GENERATION OF WEB THREATS

### Contact ScanSafe

ScanSafe US  
185 Berry Street  
San Francisco, CA 94107

T: 415 692 2000  
F: 415 536 5949  
E: [info@scansafe.com](mailto:info@scansafe.com)

### ScanSafe EMEA

The Connection, 198 High Holborn  
London WC1V 7BD

T: 020 7959 0630  
F: 020 7959 0631  
E: [info@scansafe.com](mailto:info@scansafe.com)

### About ScanSafe

Founded in 1999, ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

For more information visit [www.scansafe.com](http://www.scansafe.com)