websense®


websense® TRITON™

# TABLE OF CONTENTS


Executive Summary 3
- About The Report 5

Web Threats 6
- Legitimate Sites Serving Malware 9
- Malware Hosting 10
- Web Threat Victims 11
- Security Blog Highlights 11

Social Media Threats 12
- Shortened Web Links 14
- Twitter 14
- Facebook 15
- Security Blog Highlights 16

Mobile Threats 17
- Malicious Apps 19
- Social Risks 21
- Security Blog Highlights 22

Email Threats 23
- Changing Methods 25
- Spam: More Than a Nuisance 26
- Security Blog Highlights 28

Malware Behavior 29
- Malware Communications 31
- Rogue Anti-Virus (AV) 33

Data Theft/Data Loss 35
- Personally Identifiable Information (PII) 37
- Intellectual Property (IP) 38
- The Insider Threat 38

Conclusion 40

Appendix A 42
- The Seven Stages of Advanced Threats

Appendix B 46
- The 2013 Security Predictions Report

About Websense 48


# Executive Summary

Last year put 'trust' to the test. Can mobile devices be trusted on the network? Can users trust IT to protect them from the latest exploit? Can IT trust users to access social media safely? Can businesses trust their current defenses to protect against emerging threats? The evidence collected by Websense® Security Labs™ researchers suggests that for many organizations the answer to these questions is no. Explosive growth in several key indicators of global online criminal activity points to a *crisis of trust,* in fact, as we question the viability of "standard" security practices that have served us well over the past decade.

Cyberthreats broke new ground with mobile devices, while reaching deeper into social media. Online criminals also stepped up attacks via email, web and other traditional vectors. Our researchers measured a nearly 600 percent increase in the use of malicious web links, representing over 100 million new global malicious websites. More alarming was the news of CISOs reporting that most threats bypassed their traditional controls,[1] and they feel unprepared to meet emerging threats such as spear-phishing.[2]

This report focuses on significant changes in the global threatscape during the year, offering insights from several perspectives. Our goal is to help security professionals improve the effectiveness of existing security solutions, and identify and prioritize security gaps that may require new approaches and more innovative strategies.

1. **Web Threats.** The web became significantly more malicious in 2012, both as an attack vector and as the primary support element of other attack trajectories (e.g., social, mobile, email). Websense recorded a nearly 6-fold increase in malicious sites overall. Moreover, 85 percent of these sites were found on legitimate web hosts that had been compromised.

Number of malicious sites grew nearly **600%**

2. **Social Media Threats.** Shortened web links—used across all social media platforms—hid malicious content 32 percent of the time. Social media attacks also took advantage of the confusion of new features and changing services.

**85%** of malicious sites were found on legitimate web hosts.

[1] IDC Threat Intelligence Update, Feb. 14, 2012

[2] Websense Security Labs blog, Oct. 9, 2012, http://community.websense.com/blogs/securitylabs/archive/2012/10/09/what-is-scaring-businesses-the-most-spear-phishing-new-websense-security-labs-research.aspx

## Executive Summary (continued)

**3. Mobile Threats.** A study of last year's malicious apps revealed how they abuse permissions. Especially popular was the use of SMS communications, something very few legitimate apps do. Risks also increased as users continued to change the way they used mobile devices.

**4. Email Threats.** Only 1 in 5 emails sent was legitimate, as spam increased to 76 percent of email traffic. Phishing threats delivered via email also increased.


**5. Malware Behavior.** Cybercriminals adapted their methods to confuse and circumvent specific countermeasures. Fifty percent of web-connected malware became significantly bolder, downloading additional malicious executables within the first 60 seconds of infection. The remainder of web-connected malware proceeded more cautiously, postponing further Internet activity by minutes, hours or weeks, often as a deliberate ruse to bypass defenses that rely on short-term sandboxing analytics.


**6. Data Theft/Data Loss.** Key changes in data theft targets and methods took place last year. Reports of intellectual property (IP) theft increased, and theft of credit card numbers and other Personally Identifiable Information (PII) continued to grow. Hacking, malware and other cyberthreats continued to be a common method of attack.

Taken together, these indicators made it clear that those who treat mobile threats, email threats, web threats and other cyberthreats as separate and distinct risks will be left behind. Solutions that focus solely on mobile, email, web or otherwise can no longer be trusted to defend against complex, multistage attacks that can move between attack vectors.



## About The Report

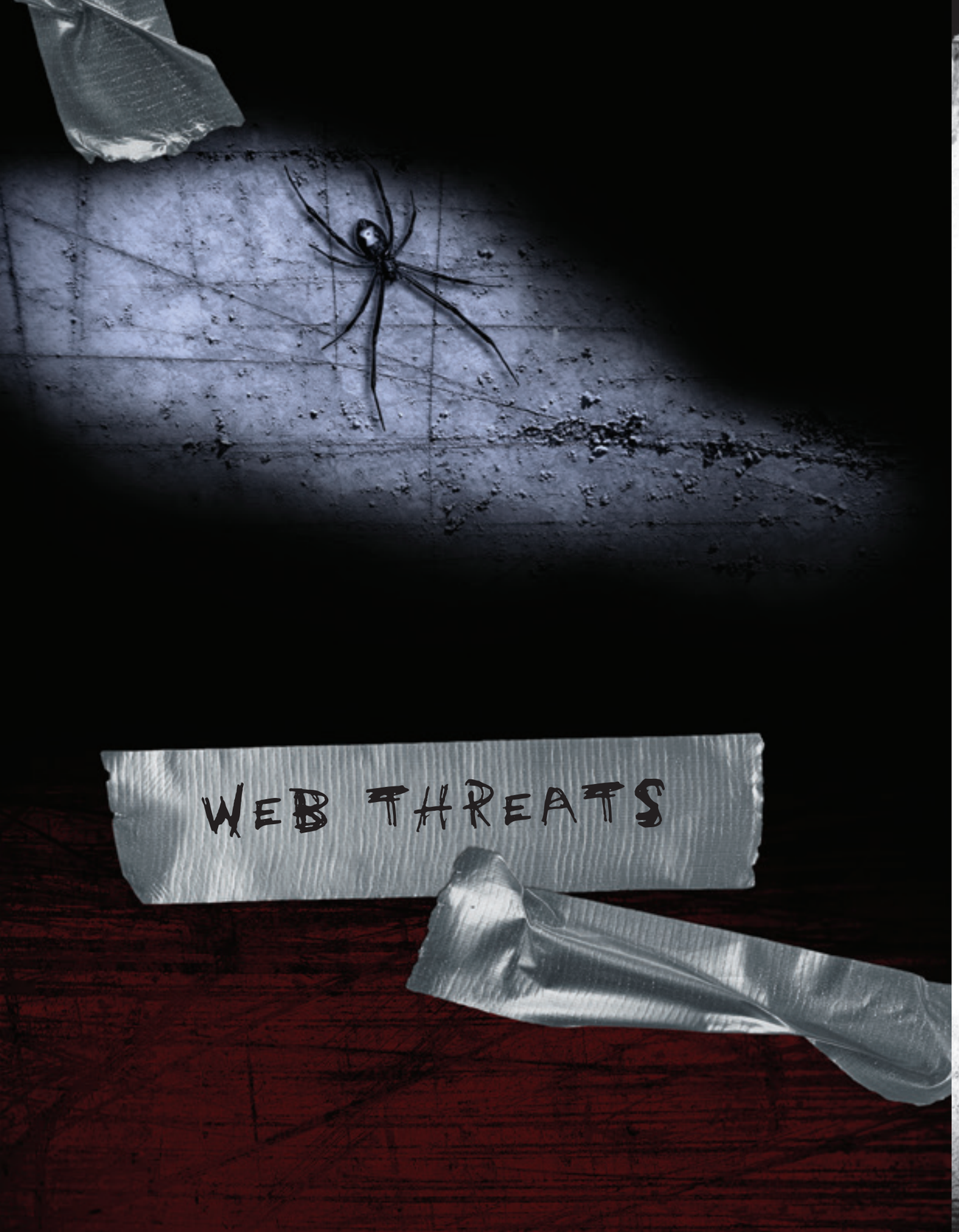
The primary source of data for this report was the Websense ThreatSeeker® Intelligence Cloud, composed of "big data" clusters used by Websense Security Labs to collect and manage up to 5 billion inputs each day from 900 million global endpoints. The world's largest threat intelligence network, the ThreatSeeker Intelligence Cloud provides visibility into real-time threat activity, including threats occurring within encrypted social media systems and other secured networks.

Data retrieved by the ThreatSeeker Intelligence Cloud was analyzed in real-time by Websense ACE (Advanced Classification Engine). With over 10,000 analytics, the result of years of research and development, ACE applies composite risk scoring to combine classifier results for real-time security, data and content analysis, and to identify key threat traits and previously unclassified zero-day exploits. ACE is also the primary engine behind all Websense TRITON™ solutions.

Websense Security Labs researchers also used Websense ThreatScope™, an online malware sandbox environment powered by ACE, to activate malware and compile an extensive report of observed behavior. ThreatScope is also available to assist Websense customers with their own forensic investigations.

The report includes analysis of the primary attack vectors of modern threats through the web, email, social media and mobile devices. Because today's complex, blended threats often involve multiple stages, our threat analysis included research into each of the seven stages of advanced threats, a summary of which is included in Appendix A.

The results of data collection and analysis were interpreted and prepared by researchers of the award-winning Websense Security Labs, with 24/7 operations in the Americas, Europe, Middle East, Africa and Asia Pacific.




## Key Finding

The number of malicious web links grew by almost 600 percent worldwide.

## Key Concept

Most malicious web links were found on hosts shared with legitimate websites, indicating that no website can be trusted—regardless of its reputation or standing.

## Key Takeaway

The web is both an attack vector and support for other attack vectors. Traditional anti-virus and firewall defenses can no longer be trusted to prevent these web-borne threats. CIOs and security personnel must adopt inline, real-time defenses that can identify if a legitimate site is still safe, or if it has been recently compromised.

# Web Threats

The web provides the foundation for the majority of threats, including attacks though mobile, email, social media or other vectors. This section reviews data that relates to the two attack functions of the web:

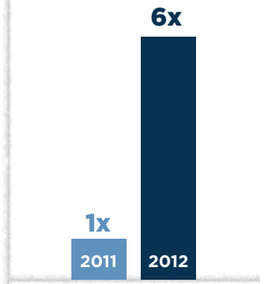
1. **The web is an attack vector.** Thanks to typosquatting and other techniques, users may first encounter an attack while surfing the web.

2. **The web supports other attack vectors.** Links sent through vectors such as social media, mobile devices or email use the web for complex evasion and attack functions.

A primary indicator of overall cyberthreat activity is the number of malicious web links that appear, and last year the amount grew by nearly 600 percent worldwide—far outpacing many traditional defenses. At the same time social media, email and other popular sites began using encrypted protocols (e.g., SSL, TLS) with greater frequency, creating blind spots for many web security solutions.

Researchers had expected a significant increase in threats. The number of Internet users has grown worldwide, web connectivity among mobile devices has exploded, and social media services have expanded as well. But a nearly 6x increase is unprecedented. In addition, as other data corroborates, it indicates that cybercriminals increased their activity in other areas as well.

Growth of Malicious Web Links 2011–2012




Source: Websense Security Labs 2012 Research.

While the amount of growth was higher in North America than in other regions (see map), the news is sobering for CISOs and security personnel everywhere. Organizations can no longer dismiss malware threats as solely an English-language or American phenomenon. For the past few years, Websense, industry analysts and others have been sounding the alarm: cybercriminals are creating increasingly targeted attacks. In fact, data from the ThreatSeeker Intelligence Cloud indicates cybercriminals are using local languages and events to target businesses and users in specific regions or areas.

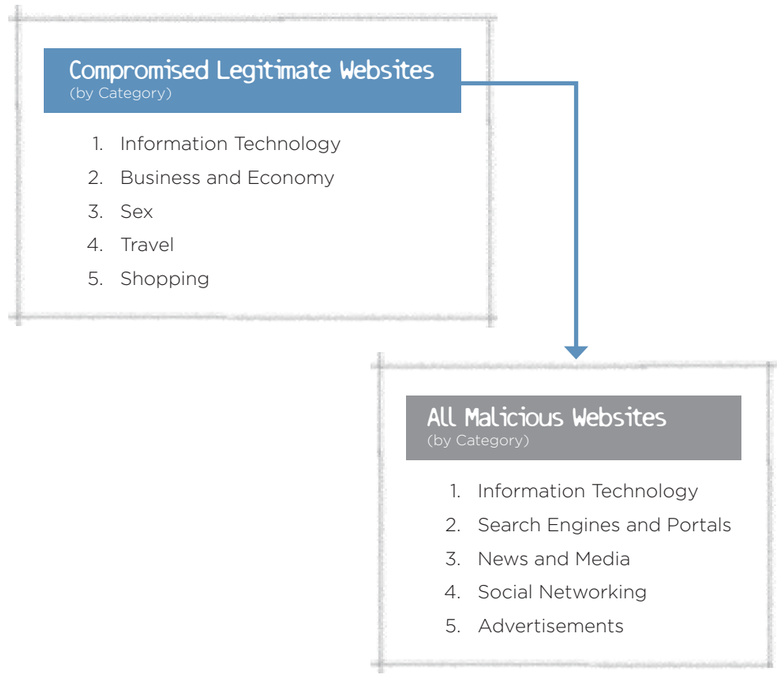
Growth of Malicious Web Links by Region 2011–2012


Source: Websense Security Labs 2012 Research.



## Legitimate Sites Serving Malware

Last year, 85 percent of malicious web links were found on legitimate hosts that had been compromised, an increase over the 82 percent found in the prior year. So the days of blocking porn and gambling websites to sufficiently mitigate web threats are long gone. Cybercriminals have switched tactics. They now target legitimate websites within categories that few organizations can restrict or block access to without affecting productivity.




Source: Websense Security Labs 2012 Research.

This shift in attack strategy is a primary reason why many traditional defenses are increasingly ineffective. IDC and other analysts reported at the beginning of 2012 that signature-based defenses were unable to address emerging threats, and the data indicates that things only got worse as the year progressed.[3] To combat such threats, CISOs and security personnel must adopt inline, real-time defenses that can identify if a legitimate site is still safe, or if it has been compromised.

[3] IDC Threat Intelligence Update, Feb. 14, 2012

## Malware Hosting

Government regulations, ISP controls, connectivity and other factors influence how cybercriminals use certain countries in different aspects of their attack plans. For example, to target victims in Brazil a cybercriminal might find it easier to set up phishing websites in the United States, send spam from Germany, host malware in Russia and establish a command and control (CnC) server in China. Websense Security Labs scrubbed ThreatSeeker Intelligence Cloud data to track these country-level trends.

### Top 10 Countries Hosting Malware


Source: Websense Security Labs 2012 Research.

## Web Threat Victims

Last year, cybercriminals increasingly set their targeted attacks on businesses and governments. For example, about 70 percent of Websense customers in both sectors experienced a weekly average of 1,719 attacks per 1,000 users. These attacks included web threats initiated through social media, mobile devices, email and other attack vectors.

The reasons cybercriminals choose a particular organization are many and varied; for example, an organization's industry, location, newsworthiness or customers are all potential factors in a cybercriminal's choice of target. Our researchers identified the top 10 "victim" countries that cybercriminals targeted, both globally and according to region.

### Worldwide: Top 10 "Victim" Countries


### EMEA: Top 10 "Victim" Countries

1. France
2. United Kingdom
3. Italy
4. Turkey
5. Germany
6. United Arab Emirates
7. Egypt
8. Macedonia
9. Sweden
10. Norway

### APAC: Top 10 "Victim" Countries

1. China
2. India
3. Taiwan
4. Philippines
5. Republic of Korea
6. Australia
7. Hong Kong
8. Vietnam
9. Singapore
10. Malaysia

### CALA: Top 10 "Victim" Countries

1. Mexico
2. Brazil
3. Argentina
4. Chile
5. Colombia
6. Peru
7. Costa Rica
8. Ecuador
9. Guatemala
10. Panama

Source: Websense Security Labs 2012 Research.

### Security Blog Highlights

> "Sharing the Experience of Deobfuscating a Trojan" http://wb-sn.com/XO0aFS

> "The Rise of a Typosquatting Army" http://wb-sn.com/11uEXU3

> "The Strange Case of the inte1sat Domain Name" http://wb-sn.com/WkhHts

> "Long Live the Injection, and How it Affects YOU!" http://wb-sn.com/WkhMxe


## Key Finding

Thirty-two percent of malicious links in social media used shortened web links.

## Key Concept

Social network popularity skyrocketed, expanding greatly into multi-lingual, international audiences. Rapidly changing feature sets often confused users, making them more susceptible to threats.

## Key Takeaway

As social media use increased in the workplace, so did the exposure of sensitive information. Trusted security solutions failed to control both inbound and outbound threats in the face of on-site, remote and mobile user access, driving IT to look at broader, more integrated options.

# Social Media Threats

Social media risks expanded as more users became "always connected" to their social networks through their omnipresent mobile devices. One study concluded that mobile devices were used 50 percent more often to access social media than to make a phone call.[4] This created an atmosphere of familiarity in which users lowered their guard, causing many to miss clues—such as shortened web links—that could indicate potentially malicious content.

The highly competitive social media market also saw the introduction of dozens of new features and capabilities across all popular platforms. It tended to confuse users, making them unaware of—and even disinterested in—how to protect their accounts or safely use the new features. This pushed even more responsibility on to IT departments, network security systems and policies to keep users and organizations secure.

## Shortened Web Links

The ability to use shortened web links in messaging, which is especially useful in space-constrained formats such as Twitter, has been around for several years. Cybercriminals often use this tactic to confound low-end web filter solutions.

Link shortening also allows cybercriminals to overcome a "side effect" of using compromised hosts for their cyberattacks. For example, to avoid detection cybercriminals try to minimize any malicious activity on popular pages of the host. Therefore, once they gain access to a host they typically hide their own malicious pages deep in the directory tree. This process generates very long and complex web links that might tip off a wary user. Link shortening solves that problem.

Of all tweets that contained web links, malicious and otherwise, 18 percent contained shortened web links. Their use is relatively small on Facebook, measuring only 1.5 percent of all posted web links. However, when we examined the posting, sharing and tweeting of malicious web links across all social networks, shortened web links disguised a malicious web page 32 percent of the time.

## Twitter

Twitter exhibited the highest use of shortened web links to spread malicious threats. And although the number of Twitter users in the U.S. remained relatively flat, total users grew to more than 500 million worldwide with rapid growth in international markets such as Brazil and Indonesia.

### Twitter Usage[5]
(by Country)

1. United States
2. Brazil
3. Japan
4. United Kingdom
5. Indonesia
6. India
7. Mexico
8. Canada
9. Spain
10. Philippines

As you would expect, Twitter's enormous popularity with users made it a popular vector for malicious attacks. However, its space and format constraints limited how creative cybercriminals could get with it. As a result, a typical malicious "tweet" last year was simply a lure designed to trick users into visiting a web page that would deliver the most malicious part of the attack. These web pages were often legitimate sites that cybercriminals had compromised to avoid suspicion and evade detection—and they were often the destination of lures sent via other social networks or other vectors such as email.

## Facebook

Facebook grew to over 1 billion subscribers last year. It continued to dominate the global social networking market, making it a prime attack vector for cybercriminals.

As a Websense strategic partner and contributor to the Threatseeker Intelligence Cloud, Facebook routinely provides Websense Security Labs with samples of suspicious content and postings for ThreatScope analysis.

[4] FactsMark Authority, July 24, 2012, http://www.factsmark.com/the-call-usage-decline-in-smartphones/

[5] CheckFacebook.com – Jan. 10, 2013, http://www.checkfacebook.com

## Facebook (continued)


### Facebook Usage[6]
(by Country)

1. United States
2. Brazil
3. India
4. Indonesia
5. Mexico
6. United Kingdom
7. Turkey
8. Philippines
9. France
10. Germany

Based on these samples, Websense has determined that security within Facebook is relatively effective overall, and few threats actually reside within the giant social network itself. However, the site is a rich target for cybercriminals, who introduce several hundred new malicious web links into Facebook daily for sharing among its 1 billion users. In total, several thousand malicious web links circulate daily.

### Security Blog Highlights

- "Beware of Scams Related to Facebook Timeline!" http://wb-sn.com/14vDAId
- "Weibo Accounts Compromised to Spread Phishing Campaign" http://wb-sn.com/11uFAgC
- "Pinning Down Pinterest" http://wb-sn.com/Xudjph
- "Social" malware ready for the Olympic Games 2012" http://wb-sn.com/11uFS6V
- "Pak Hack Attack: Pastebin Reveals Attacks" http://wb-sn.com/UKGZA2
- "Christmas-Themed Facebook Scams: How Cybercrooks Kick it up a Notch and Piggyback on Big Brands" http://wb-sn.com/WGgVUe

[6] Techcrunch – July 30, 2012 - "Analyst: Twitter Passed 500M Users In June 2012, 140M Of Them In US; Jakarta 'Biggest Tweeting' City"- http://techcrunch.com/2012/07/30/analyst-twitter-passed-500m-users-in-june-2012-140m-of-them-in-us-jakarta-biggest-tweeting-city/



## Key Finding

Eighty-two percent of malicious apps sent an SMS message as part of their attack, something very few legitimate apps ever do.

## Key Concept

Data stored on a mobile device, and data accessed through the device, are at risk due to minimal control of web, email and social media traffic and access. Lost devices are also a risk.

## Key Takeaway

How mobile devices are used and attacked is continuing to erode IT's ability to trust solely in mobile device management (MDM). Security teams need to supplement MDM with defenses capable of limiting mobile access to key resources, and performing real-time analysis of potentially malicious content in mobile web, email and social media traffic.



# Mobile Threats

Even though lost mobile devices continue to pose a major security problem, malicious apps and social media threats emerged as the dominant security issues. In fact, the risk of losing confidential data through mobile devices moved from proof of concept to reality in the past year. An explosion of apps, devices and technological advances provided new opportunities to create exciting legitimate applications and services—but also inspired new malicious activity.

The jailbreaking of mobile devices remained popular, and therefore malicious apps continued to threaten these devices. However, malicious apps increasingly threatened unmodified mobile devices as well by appearing in legitimate apps stores, hidden among the hundreds of new apps submitted daily.

Legitimate apps were also a cause for concern; many proved less secure than expected. Consider a study by Philipps University and Leibniz University in Germany involving 13,500 free apps downloaded from Google Play. Researchers found that 8 percent of these apps were vulnerable to man-in-the-middle attacks, and approximately 40 percent enabled the researchers to "capture credentials for American Express, Diners Club, Paypal, bank accounts, Facebook, Twitter, Google, Yahoo, Microsoft Live ID, Box, WordPress, remote control servers, arbitrary email accounts, and IBM Sametime, among others."[7]

Of course, all things mobile will only get better and worse, because the same technological advances that hold great promise for users will also benefit cybercriminals. Innovations such as hosted virtual desktops, HTML5, silicon-anode batteries, media tablets and cloud-based computing will enable new capabilities that developers of both legitimate and malicious apps can exploit.[8]

## Malicious Apps

Ensuring that apps are safe remains a primary objective of legitimate app stores. Nonetheless, last year we saw these trusted sites increasingly breached as malicious apps appeared more frequently.[9] As both Apple and Google app stores surpass one billion apps, the likelihood of more malicious apps slipping through the cracks will only increase.

A technique to help users pirate mobile apps, jailbreaking dramatically increases the risk of malware infecting a mobile device. As many as one million devices were jailbroken in just the first weekend of a new OS release in 2012.[10]

In short, mobile apps can no longer be trusted—not without careful scrutiny of their behavior.

[7] Oct. 2012, "Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security," http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf

[8] Gartner press release, Aug. 16, 2012, http://www.gartner.com/newsroom/id/2124315

[9] Wired, "First Instance of iOS App Store Malware Detected, Removed", July 5, 2012, http://www.wired.com/gadgetlab/2012/07/first-ios-malware-found/

[10] iDownloadBlog, May 28, 2012, http://www.idownloadblog.com/2012/05/28/absinthe-2-0-provesjailbreaking-is-as-popular-as-ever/

## Malicious Apps (continued)

Many articles and presentations last year recommended, as a proactive defense, that users carefully review the permissions that apps require before installing them. Yet few provided details about which permissions are safe, which are dangerous and which are typical of legitimate apps. Websense Security Labs reviewed the permission requirements of malicious apps in our library against the permissions of legitimate apps that are currently available. Because iOS does not expose permission requirements to users, we restricted this study to Android apps—but we believe the results reflect iOS threat activity as well.

### Permission Exploitation

| Malicious APP | Android Permission Type | Legitimate APP |
|---|---|---|
| 1 | INTERNET | 1 |
| 2 | READ_PHONE_STATE | 3 |
| 3 | SEND_SMS | X |
| 4 | WRITE_EXTERNAL_STORAGE | 4 |
| 5 | ACCESS_NETWORK_STATE | 2 |
| 6 | RECEIVE_SMS | X |
| 7 | READ_SMS | X |
| 8 | RECEIVE_BOOT_COMPLETED | 11 |
| 9 | CALL_PHONE | 17 |
| 10 | WAKE_LOCK | 9 |
| 11 | ACCESS_COARSE_LOCATION | 6 |
| 12 | VIBRATE | 8 |
| 13 | RECEIVE_WAP_PUSH | X |
| 14 | ACCESS_FINE_LOCATION | 7 |
| 15 | WRITE_SMS | X |
| 16 | ACCESS_WIFI_STATE | 5 |
| 17 | GET_TASKS | 10 |
| 18 | SET_WALLPAPER | 14 |
| 19 | READ_CONTACTS | 15 |
| 20 | INSTALL_PACKAGES | X |

X Indicates that the permission is not among the top 20 permissions used in legitimate apps.

Source: Websense Security Labs 2012 Research.

You can see in the table that malicious apps used mostly the same permissions as legitimate apps. In addition, we saw three interesting permission requirements among malicious apps that are worth pointing out:

1. Eighty-two percent of malicious apps send, receive, read or write SMS messages. Very few legitimate apps require any SMS permissions.
2. One in eight malicious apps required RECEIVE_WAP_PUSH permission, something legitimate apps rarely require.
3. One in 10 malicious apps asked for permission to install other apps—another rarity among legitimate apps.

Note: There *are* legitimate reasons that a legitimate app may require any of these rarely used permissions, so none is a reliable indicator of a threat. However, any app that requests any of these permissions should be examined more closely to see if the permission request makes sense. In addition, it's useful to know how legitimate apps behave, as a starting point to differentiate between acceptable and suspicious app behavior. For example, an increasing number of legitimate apps require web-access permissions for a number of reasons: to support a social media feature; to serve advertisements in free apps; to use web-based information such as news, weather or sports scores; etc.

## Social Risks

### How Smartphones are Used[11]


[11] FactsMark Authority, July 24, 2012, http://www.factsmark.com/the-call-usage-decline-in-smartphones/

## Social Risks (continued)

Mobility has become an integral part of our professional and personal lives, and is used for much more than just talking to other people. One study last year found that mobile users spent almost 50 percent more time using their mobile devices for social networking than for phone calls.[11]

Social media apps became even more popular, reflecting users' preference to access the web on their mobile devices. Data shows that 73.6 percent of iPhone users actively connect to Facebook using the Facebook app for iPhone, and the Android version of the app has a 30 percent higher penetration rate.[12] The number of total mobile Facebook users was 680 million.[13] As a result, all of the threats discussed earlier in the Social Web section also pose a threat to mobile devices.

It became clear last year that those who treat mobile threats, email threats, web threats and other cyberthreats as separate and distinct risks are at greater risk than those who adopt a more holistic and integrated security posture. Security solutions that focus solely on mobile, email, web threats or similarly siloed security approaches can no longer be trusted to defend against complex, multistage attacks that can move between attack vectors.

### Security Blog Highlights

- "Hook, Line and Sinker: The Dangers of Location-Based Services (LBS)" http://wb-sn.com/VAbET9
- "Watch out for Malicious UPS/FedEx Notifications When Waiting for iPhone 5" http://wb-sn.com/11uGoBV
- "The Android 'GoldDream' Malware Server is Still Alive" http://wb-sn.com/UUqNyA
- "Malicious Email MMS Targets Mobile Phone Users" http://wb-sn.com/14vDY9K

[12] TechCrunch – Jan. 4, 2013 - "Facebook Mobile User Counts Revealed: 192M Android, 147M iPhone, 48M iPad, 56M Messenger," http://techcrunch.com/2013/01/04/how-many-mobile-users-does-facebook-have/

[13] The Next Web, Jan. 30, 2012, "Facebook passes 1.06 billion monthly active users, 680 million mobile users, and 618 million daily users," http://thenextweb.com/facebook/2013/01/30/facebook-passes-1-06-billion-monthly-active-users-680-million-mobile-users-and-618-million-daily-users/



## Key Finding

Only one in five emails sent last year was safe or legitimate, and more than half of users accessed email beyond the reach of traditional defenses.

## Key Concept

Cybercriminals added a “time-delay” to some targeted attacks, in which embedded web links are kept benign until after traditional email security defenses are bypassed.

## Key Takeaway

Email-based threats evolved significantly to circumvent keyword, reputation and other traditional defenses. Trust has eroded in the face of increased spear-phishing and other legitimate-appearing messages based on sophisticated social engineering. Reliable email security requires real-time threat analysis methods that coordinate with web, mobile and other defenses.



# Email Threats

Email was a significant component of multistage attacks in all languages and in all regions last year, contributing to increased malware infections and data theft. Only one in five emails was safe or legitimate, and in a blind phishing study, Websense found that more than 50 percent of users accessed email from outside the corporate network. This may indicate that our increasingly remote and mobile workforce, beyond the safety of traditional corporate network security, is at a greater risk if they fall prey to carefully crafted social engineering ploys delivered via email.

In general, sophisticated targeted content made email a highly effective attack vector for phishing, malware and spam. Messaging was increasingly regionalized, using local brands, celebrities and events to lure users into taking actions that might expose them to further risk.

## Changing Methods

A disturbing twist on such targeted attacks emerged last year. Cybercriminals identified a major exploitable design flaw in traditional email security defenses. These defenses evaluate an embedded web link only when the email containing it enters an organization’s email system—not when the recipient clicks on it. A cybercriminal takes advantage of this security shortcoming by compromising a link’s destination web page after the web link safely gets past email security defenses—and before the recipient clicks on it—effectively adding a “time-delay” aspect to these targeted attacks.

In general, email threats adapted to numerous changes in user behavior and technology last year. During the first six months, security measures and user awareness reduced the effectiveness of traditional scams. Cybercriminals responded by using legitimate-appearing events, brands and web links in their email attacks to mask their intentions. These tactics made detection more difficult because email threats increasingly mimicked legitimate messages, from apparently legitimate sources, and often contained web links to legitimate websites that the attacker had recently compromised.

Spear-phishing increased, and many of last year’s notable attacks showed the value cybercriminals place on this technique. A spear-phishing attack begins with a cybercriminal performing online “reconnaissance” to compile information on a targeted victim’s work, education, hobbies or other interests. This allows the cybercriminal to create a personalized message that will entice the victim to act without arousing suspicion.

Attacks such as Flame[14], Zeus[15], Stuxnet[16] and Red October[17] were often delivered as the result of highly targeted spear-phishing messages sent to select individuals or groups.

[14] Websense Security Blogs, May 30, 2012, “Malware Traditions on Fire: What you need to know about Flame,” http://community.websense.com/blogs/securitylabs/archive/2012/05/30/malware-traditions-on-fire-what-you-need-to-know-about-flame.aspx

[15] Websense Security Blog, Oct. 5, 2012, “When Less is More: The Growing Impact of Low-Volume Email Attacks,” http://community.websense.com/blogs/securitylabs/archive/2012/10/05/When-less-is-more-the-growing-impact-of-low-volume-email-attacks.aspx

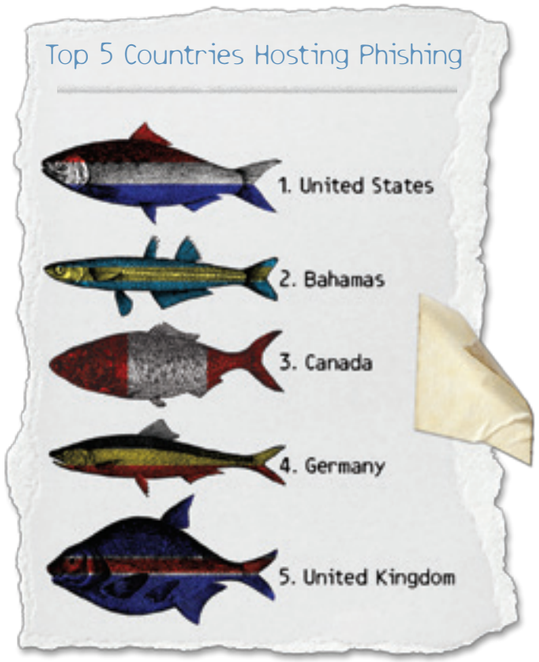
[16] Websense Security Labs Blog, Oct. 19, 2012, “Duqu - Stuxnet 2.0,” http://community.websense.com/blogs/securitylabs/archive/2011/10/19/duqu-stuxnet-2-0.aspx

[17] Websense Security Blog, Jan. 21, 2013, “The Hunt For Red October,” http://community.websense.com/blogs/securitylabs/archive/2013/01/21/the-hunt-for-red-october.aspx

## Changing Methods (continued)

Many of these attacks have a long shelf life. By constructing new emails, cybercriminals can use the same malware repeatedly for several years with only minor changes. For example, Stuxnet first appeared in 2010, yet reportedly was used as recently as December 2012 in a targeted attack on Iranian power and other industries.

There are particular factors to consider when examining phishing data. Phishing hosts shift frequently (e.g., Brazil, Egypt, Israel and other countries all appeared in the top five at various times during the year). Hosts may even change in the middle of an attack in response to obstacles, such as when a host detects unusual activity and interrupts the attack. And many attacks actually use multiple hosts, to send the most email in the shortest time.



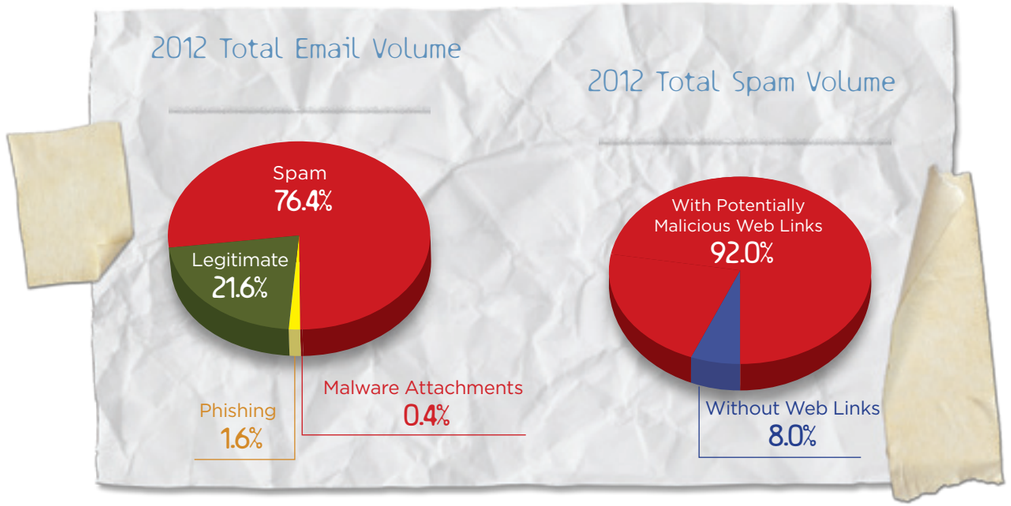

Source: Websense Security Labs 2012 Research.

One aspect of phishing attacks remained constant last year: two-thirds of phishing emails were sent on Mondays and Fridays. These are the days when users are more distracted with personal concerns, such as weekend activities, and typically have their guard down—making them more likely to fall prey to attacks.

Timeliness continued to be of the essence in successful email attacks. Scheduled events such as the Olympics provided many opportunities for abuse; for example, many email attacks took place months before the opening ceremonies, using offers of fake tickets, travel and other Olympic-related items. Unplanned events, such as a celebrity death or a natural disaster, also provided key opportunities for cybercriminals, who often reacted to such events in less than 12 hours.

## Spam: More Than a Nuisance

Global spam volume grew to 76 percent of all email, up from 74 percent in 2011 and reaching more than a quarter of a million emails sent per hour. Our key findings indicate that spam is no longer a mere nuisance—last year, 92 percent of spam email included web links that often pointed to phishing, malware and other malicious content. As shown in the following charts, relatively few emails actually contained malicious content, leading security systems that screen email based on the presence of malicious content in the email itself to typically identify 76 percent of email as harmless spam (see pie chart upper right). However, further analysis by Websense indicated a large percentage of spam (76.4 percent of all email) contained potentially malicious web links.




The spam threat is compounded by the increased use of time-delay tactics, as noted above. An email that may present itself to the user as innocuous spam or advertising content can contain web links that are switched at will from safe to compromised web pages, complicating malware detection for all but the most sophisticated security systems capable of real-time, inline sandbox execution of web links whenever they are activated by the user.

Below is a deeper analysis of the top categories of web links embedded in spam. Malicious spam is spam that contained links to web pages other than those classified as “Web and Email Spam.”

Top 5 Categories of Malicious Web Links in Spam Email

| | | |
|---|---|---|
| 1 | Potentially Damaging Content | Suspicious sites with little or no useful content. |
| 2 | Web and Email Spam | Sites used in unsolicited commercial email. |
| 3 | Malicious Websites | Sites containing malicious code. |
| 4 | Phishing and Other Frauds | Sites that counterfeit legitimate sites to elicit user information. |
| 5 | Malicious Embedded iFrame | Sites infected with a malicious iframe. |

Source: Websense Security Labs 2012 Research.

The table above shows an increase of malicious intent in spam compared to the previous year, when the No. 1 link classification in spam was in the relatively benign “Web and Email Spam” category.

## Spam: More Than a Nuisance (continued)

These are sobering facts for those who thought email threats were declining or no longer evolving alongside other cyberthreats. As with most mobile and social threats, email typically plays a more innocent-appearing role in the early stages of an attack. Its intent is to lead users to web content that carries out the most malicious activity. Spam messages often lead the user to danger, while phishing emails primarily distribute banking Trojans, backdoors and bot programs.

Today's blended email attacks often use the web to disguise their intentions, circumvent single-vector security solutions and carry out their objectives while evading detection. Trustworthy email security increasingly depends on real-time threat analysis methods that coordinate with web, mobile and other defenses.

### Security Blog Highlights

- "You may be 'Surprise too' [sic] receive this letter from me. . ." http://wb-sn.com/YJv9cJ
- "What is Scaring Businesses the Most? Spear-phishing. New Websense Security Labs Research" http://wb-sn.com/Ypyn1b
- "Phishing for Apple IDs" http://wb-sn.com/11uHqOi
- "Malicious URLs in Fake Craigslist Emails" http://wb-sn.com/WGhr4x

## Key Finding

Malware proved increasingly bold. Half of web-connected malware downloaded additional executables in the first 60 seconds of infection. The remainder of web-connected malware proceeded more cautiously—often a calculated response to bypass short-term sandbox defenses.

## Key Concept

Malware grew increasingly web-connected to make attacks more dynamic and flexible, enabling cybercriminals to evade detection and exploit unique vulnerabilities in each system they encountered.

## Key Takeaway

The days when malware occasionally communicated to CnC servers, sometimes once a day or less, are over. Today's malware is more dynamic and agile, often adapting to an infected system within minutes. In this new environment, traditional defenses are often left behind.



# Malware Behavior

When investigating attacks, Websense Security Labs researchers commonly dissect malware, scripts and other potentially malicious code. Last year, they found that malware remained at the heart of most cyberthreats, even if intended for use at a later stage of the attack.

It is important to keep malware research in perspective. For example, while threats such as Flame, Stuxnet and Zeus provide for interesting case studies and news articles, they are the exceptions, not the rule. Most threats are generated by exploit kits or based upon older malware samples. Few users will ever actually encounter a piece of "celebrity malware."

When researchers ran last year's malware collection through the ThreatScope forensic sandbox to identify common trends in malware behavior, the exercise revealed that many popular techniques of past infections are declining. For example, only 7.7 percent of last year's malware modified the System Registry. Instead, they found that behaviors increasingly used Internet resources to communicate more frequently with those orchestrating the attack. To assume a more proactive security posture, security professionals need to adjust their strategies and defenses to address these changes in attack patterns and behaviors.

## Malware Communications

Malware communicated more frequently with its controllers than in previous years, when malware might attempt to communicate only once daily, weekly or monthly to reduce the chance of detection. Malicious traffic can now travel less conspicuously as it hides among a constant flow of small data bursts from social apps, auto-refreshing web pages and mobile devices.

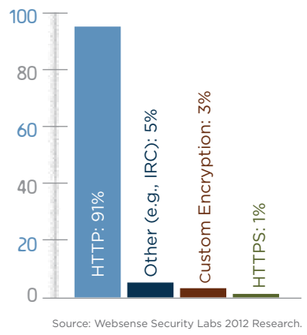
One part of our study focused on the network communications that malware performed in just the first 60 seconds. The ThreatScope forensic sandbox identified that a surprising 15 percent of malware was unafraid to reach out via the web during the first minute of infection, with 90 percent of these requesting additional guidance and information. Fifty-percent of web-connected malware downloaded additional executables, often called dropper files, in the first 60 seconds of infection.[18]

Still, some threats use more conservative methods to avoid detection by the growing number of sandbox solutions. Flame, for example, performed no function for the first 5-6 minutes of operation. This lack of activity would earn it a "safe" rating by many solutions that only monitor sandbox activity for a period of seconds, enabling the exploit to bypass defenses until it was too late to protect against them.

[18] See Appendix A

## Malware Communications (continued)

### Analysis of CnC Communication Protocol




Source: Websense Security Labs 2012 Research.

Last year, the most common malicious Internet communications happened through CnC servers that enabled cybercriminals to control infected systems and issue commands. (The widespread use of these CnC networks and their infected endpoints, known as Botnets, dates back to 2007.) We also found that CnC communications have begun to take greater measures to hide their communications from security solutions.

A quick glance at the table data might suggest that securing HTTPS should be a low priority, but that's not the case. Social media and most other popular websites increasingly use HTTPS to encrypt traffic between their services and their customers. This also allows the safe passage of malware and other threats, because it presents a blind spot to many security solutions.

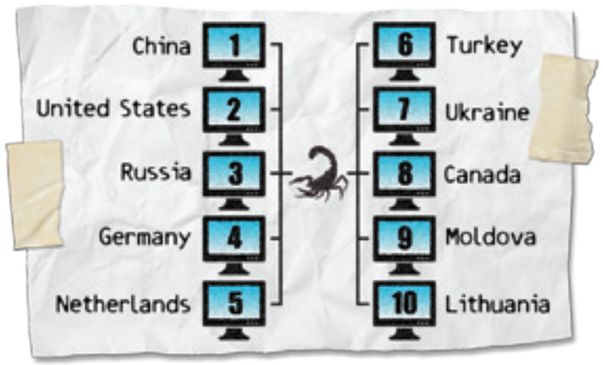
The type of CnC communications represented in the table happen only after infection. To avoid detection, such communications are typically short and contain no obviously malicious content. When something significant needs to be transmitted, such as a malware update or stolen data, these communications often use simple but proven data encryption, then send it through HTTP or another channel.

This highlights another way that threats adapt through the multiple stages of an attack. At each stage, they take advantage of the methods and technologies that enable them to successfully move onto the next stage—at which point the attack changes again.

So monitoring inbound HTTPS traffic is vital to blocking attacks even though it provides minimal value in detecting CnC communications.

As noted in the web threat section of this report, various components of today's threats may be hosted in various parts of the world. Here are the top 10 countries that hosted CnC servers last year.

### Top 10 Countries Hosting CnC Servers



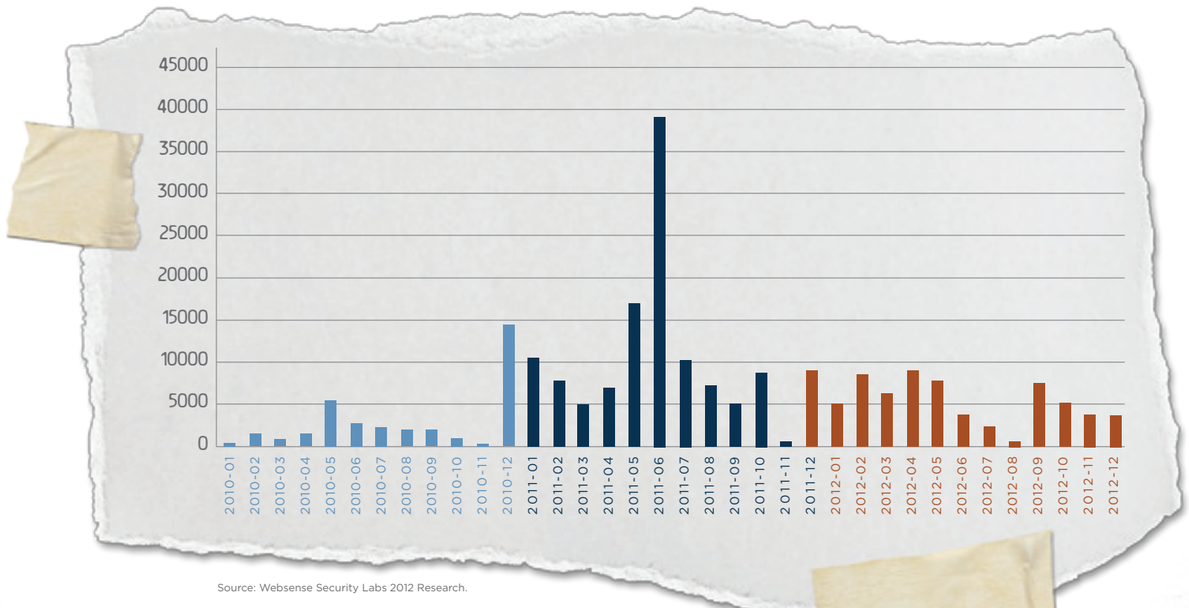

Source: Websense Security Labs 2012 Research.

Overall, malware is rarely designed to be a complete, self-contained attack vehicle. Other, more complex attack strategies have proven more popular, and as a result, sophisticated defenses are needed to contain such attacks. For example, in a simple attack, such as an email with an attachment of self-contained malware, defenses require only email threat detection or malware detection capabilities. To defend against complex attacks, defenses must have multiple layers, properly deployed and integrated across web, email, social and mobile vectors. Security personnel today can achieve this level of protection, so long as they have inline defenses that can perform real-time analysis along every attack vector, and at each layer of defense. (See Appendix A, "The Seven Stages of Advanced Threats," to learn more.)

## Rogue Anti-Virus (AV)

An important lesson about malware is that it can be persistent. Many pieces of malware that infected systems in 2012 were created in 2011 or earlier. Rogue AV, or Fake AV, is a good example of malware's longevity.

### Rogue AV Release Dates for Currently Active Threats




Source: Websense Security Labs 2012 Research.

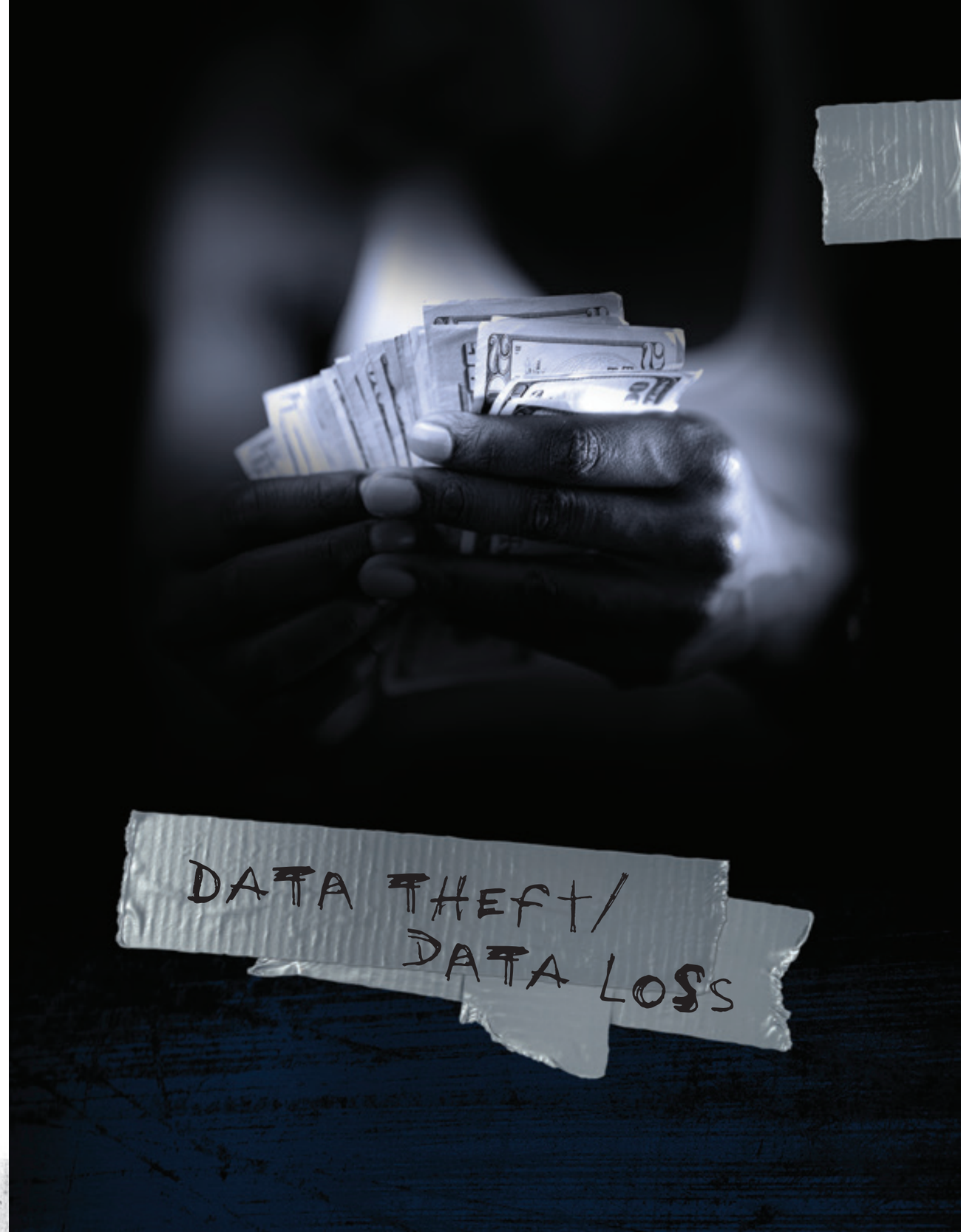
## Rogue Anti-Virus (continued)

Over 200,000 web links related to Rogue AV remained active at the end of last year, even though they were known to support fake anti-virus attacks. The primary reason the attack continues to be prevalent in corporate environments is that many inexpensive hosting services don't offer threat monitoring or scanning services.

While other recent data may indicate that malware-hosting websites are typically cleaned within a few hours, our analysis in the previous table is an important reminder that some "old" threats are still very much alive. It's a good reminder that security strategies cannot be based solely upon what is considered typical.

There is another lesson here. As our data shows, Rogue AV was a significant threat in 2010 and 2011, with infection rates declining in 2012. The significance is not that the attack became less effective, but that almost two years passed before browsers and plugins were appropriately updated and vulnerability patches were released.

Let Rogue AV serve as a case study for security planning. IT cannot depend on vendor patches and other outside measures to secure their networks or protect their mobile and remote workers. As noted above and in Appendix A, integrated, layered defenses require real-time analysis capabilities to identify threats and provide defenses where they are needed, in real time.



## Key Finding

Planned data theft attacks through cyberspace grew last year, targeting high value intellectual property (IP) and using all available vectors.

## Key Concept

Execution of well-planned attacks on IP increased while reports of lost devices containing Personally Identifiable Information (PII) declined.

## Key Takeaway

The insider threat grew as personnel became increasingly mobile, and tools to empower them with easier access to information were deployed. Measures must be taken to reinstate trust in personnel, and in the organization's ability to police and protect its most valuable data. IT can remove temptation and mitigate accidental loss through security improvements that address growing SSL/TLS usage, and provide an integrated approach to monitoring and controlling both inbound and outbound content.



# Data Theft/Data Loss

Intentional, well-planned cyberattacks by outsiders increased last year, while major data loss through the theft or accidental loss of laptops, backup tapes and other data repositories continued to decline. The insider threat also grew as personnel and contractors took advantage of encrypted communications (e.g., SSL, TLS), a rising blind spot for security solutions as email, social media and other popular sites and services began to use these encryption protocols.

Data theft attacks targeted IP ranging from government secrets to household appliances and toys. The increased interest in IP did not reduce efforts to steal credit card numbers and other PII. Some security breaches uncovered appeared to have been operating for several years.

## Personally Identifiable Information (PII)

The markets to sell PII are well established,  making attacks lucrative and easy to monetize. And while regulatory pressure is continuing to build throughout the world for greater PII controls, incidents continue to be uncovered at a dizzying pace, resulting in significant repercussions for organizations breached—and often for those who do business with them.

A 2012 credit card breach at Global Payments, a third party credit card processor, affected Visa, MasterCard, American Express and Discover.[19] One of the largest credit card thefts in recent years, it was on scale with the Heartland Payment Systems breach of 2008.[20] Fortunately, based on lessons learned from other attacks, Global Payments was able to respond and contain the breach quickly.[21] Unfortunately, the credit card companies that relied on Global Payments watched their stock values plummet as news of the attack spread. Some cancelled their contracts with Global Payments to regain the confidence of their own customers.

Financial institutions were not the only victims of attacks on PII. An attack on Zappos.com, a popular retail shoe website, exposed customer data stored on the company's internal network and systems, placing 24 million accounts at risk.[22]


Secret Service probes major credit card breach

Reuters / March 31, 2012

The U.S. Secret Service is investigating a major cyber intrusion at an Atlanta-based payment processor that could expose millions of MasterCard, Visa, American Express and Discover cardholder with fraudulent charges. Processor Global Payments Inc. said on Friday it had found "unauthorized access" into its system early in March and notified law enforcement and financial institutions.

Payment network operators confirmed they were affected, along with banks and other financial firms that issue credit cards to consumers.

[19] Forbes, Apr. 1, 2012, "Global Payments Pegs Security Breach At 1.5 Million Credit Cards As Visa Decertifies Processor Firm," http://www.csmonitor.com/Business/Latest-News-Wires/2012/0331/Secret-Service-probes-major-credit-card-breach?nav=topic-tag_topic_page-storyList

[20] Wikipedia, http://en.wikipedia.org/wiki/Heartland_Payment_Systems

[21] Reuters, June 12, 2012, "Global Payments says data breach is 'contained'", http://www.reuters.com/article/2012/06/12/us-globalpayments-breach-idUSBRE85B1IC20120612

[22] International Business Times, Jan. 16, 2012, "Zappos Hacked, 24 Million Users' Data Stolen: How to Protect Your Account Information" http://www.ibtimes.com/zappos-hacked-24-million-users%E2%80%99-data-stolen-how-protect-your-account-information-395962

## Personally Identifiable Information (PII) (continued)

Government agencies also continued to fall victim to these attacks, even as they imposed new regulations and higher penalties on the private sector for similar breaches.[23] For example, in November 2012, a 35 year-old man obtained PII on what could represent 80 percent of the population of Greece.[24]

## Intellectual Property (IP)

IP came under increasing attack last year, even as organizations tried to keep data breaches confidential to avoid negative publicity and its impact on stock values or customer confidence. The U.S. Joint Economic Committee in August issued a report about the potential impact of stolen IP, saying that as a result, "counterfeiting and piracy have become increasingly widespread."[25]


IP breaches uncovered during the year indicate that intentional acts by employees are on the rise. While most security measures to protect PII may also help secure IP, organizations still need to reevaluate internal processes, procedures and controls in light of this trend. They must address the insider threat to ensure employees can be trusted to access the information required to perform their job functions.

## The Insider Threat

Despite efforts to strengthen defenses, control unsecured devices, restrict the usage of social networks, and otherwise mitigate the risk of cyberattack, users remain the weakest link in information security. Unaware that a friend's account might have been compromised, for example, users may follow web links on social networks or in email simply because they trust the sender. Phishing emails and websites use social engineering ploys to trick users into revealing sensitive information, while malware and malicious apps often capture user credentials. The opportunities to take advantage of network users are many and varied.

[23] BBC News, Jan. 25, 2012, "EU data protection law proposals include large fines", http://www.bbc.co.uk/news/technology-16722229

[24] InfoSecurity, Nov. 22, 2012, "Greek man arrested over theft of 9 million personal data details", http://www.infosecurity-magazine.com/view/29469/greek-man-arrested-over-theft-of-9-million-personal-data-details/

[25] JEC press release, Aug. 6, 2012, http://www.jec.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=a3e1248a-012f-4837-897e-7a884414a911



IP doesn't just involve data on medical breakthroughs or military secrets, as depicted in so many Hollywood movie plots, for cybercriminals to consider them valuable. In the toy industry, for example, a blogger was sued last year for leaking information about unreleased Nerf products.[26]

Other events reveal the extent to which many will go to steal IP. Late last year, vacuum cleaner manufacturer Dyson filed a lawsuit against its competitor Bosch for allegedly planting a "mole" within Dyson with the intent to steal the company's IP.[27]

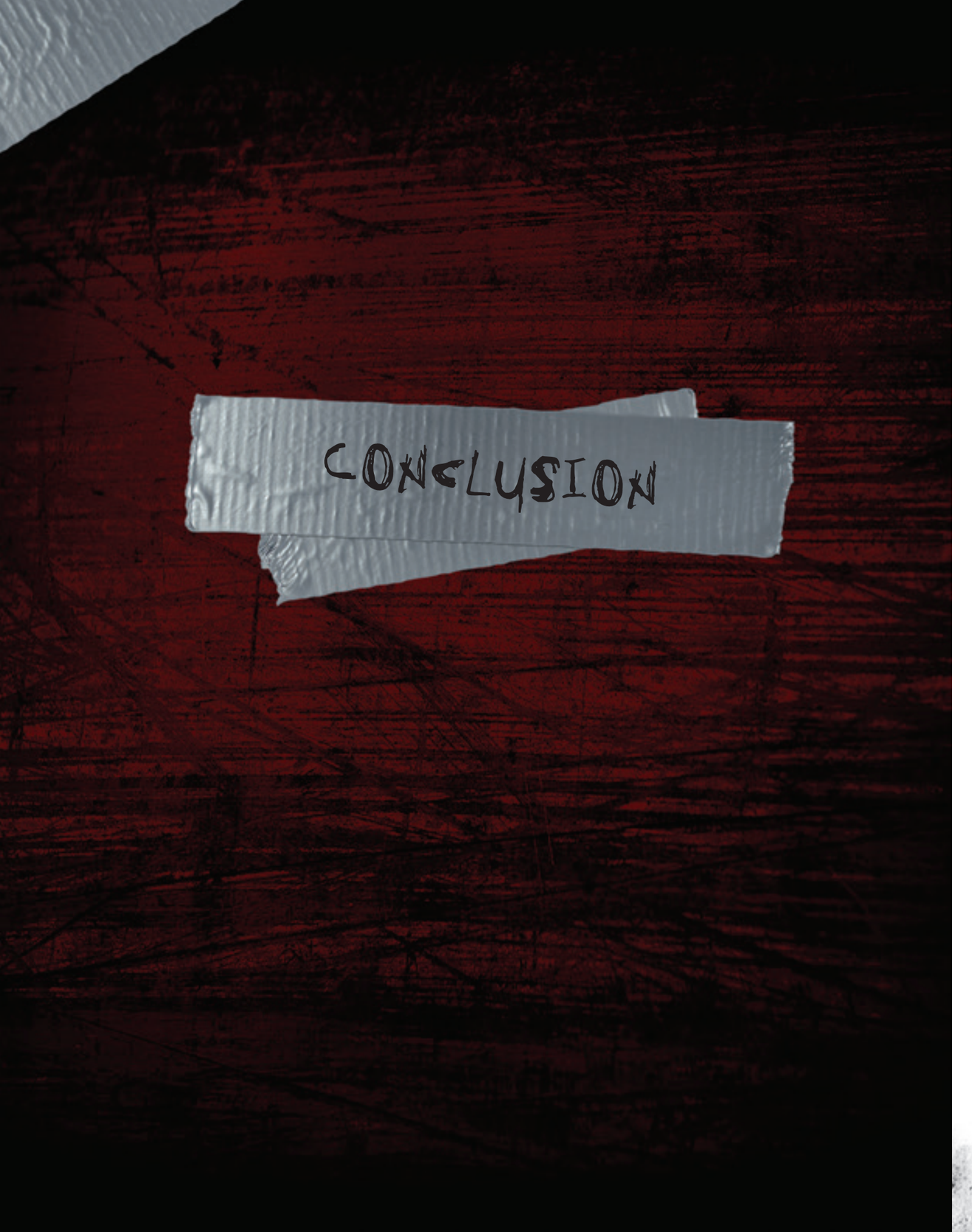
Even agencies devoted to security can fall victim. Counter-terrorism secrets shared by foreign governments may have been compromised by a massive data theft perpetrated by a senior IT technician for the NDB, Switzerland's intelligence service.[28]

From games to governments to household appliances, all IP is valuable to someone. Organizations need to consider new security measures, such as restricting some data on non-mobile devices. Features once considered "nice to have," such as securing USB drives or monitoring for encrypted traffic and files, are now considered "must haves" for retaining trust in organizations' ability to balance productivity with security.


[26] Techcrunch, Apr. 25, 2012, "Hasbro Goes After Blogger In IP Theft Case", http://techcrunch.com/2012/04/25/hasbro-goes-after-blogger-in-ip-theft-case/

[27] Reuters, Oct. 24, 2012, "UK's Dyson accuses Germany Bosch of paying "mole" for tech info", http://www.reuters.com/article/2012/10/24/dyson-mole-idUSL5E8LOG8H20121024

[28] Reuters, Dec. 4, 2012, "Swiss spy agency warns U.S., Britain about huge data leak", http://www.reuters.com/article/2012/12/04/us-usa-switzerland-datatheft-idUSBRE8B30ID20121204




The Websense 2013 Threat Report confirms that cyberattacks escalated on every front and through every vector last year, straining every layer of enterprise defenses. Moreover, cybercriminals are already swiftly exploiting the latest advancements in mobile devices, social media and other technologies to advance their art and take an ever-greater toll on legitimate commerce.

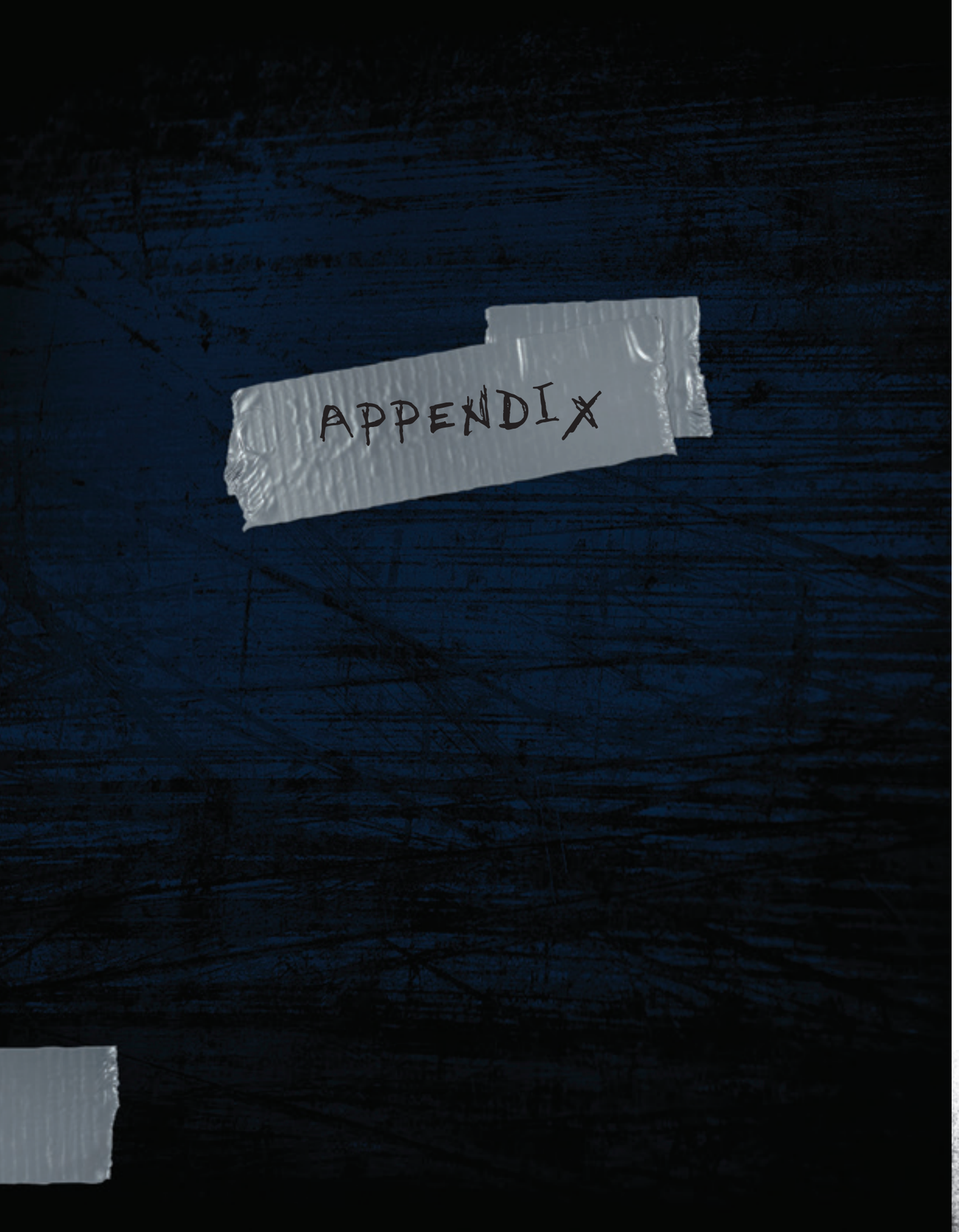
While security strategies must turn to tighter controls on email, mobile devices and social media, the heart of almost all attacks through these vectors continues to be the web. Regardless of the lures sent through other channels, these attacks all use the web to enhance their social engineering efforts and hide their true intent while waiting for the right moment to install malware, communicate with a CnC server or deliver stolen information. Every industry, region and language saw dramatic growth in malicious web activity as the common conduit through which cybercriminals perpetrated email, mobile and social media attacks.

Cybercriminal activity last year also showed highly evolved attack strategies designed to work across multiple attack vectors, in multiple stages, and often launched from multiple geographies, to evade conventional defenses and provide redundancy and scale to their attacks. Attacks were also more patient as they sought out high value information, progressing in stages, and quickly adapting when detected.

Taken as a whole, the data makes it clear: organizations that treat mobile threats, email threats, web threats and other cyberthreats as separate and distinct risks leave themselves unprotected against highly sophisticated, blended attacks coordinated across multiple vectors. Moving forward, effective protection will be predicated on inline, real-time defenses that are unified across attack vectors.

Based on this report's findings, Websense suggests that information security professionals and decision makers consider the following when planning their defenses:

1. Inline, real-time information security is necessary to help prevent web-borne threats.
2. Integrated security solutions are required to control inbound and outbound threats brought about through increasing use of social media by on-site, remote and mobile users.
3. Mobile device management (MDM) capabilities must be augmented with defenses that can control mobile access to key resources, and perform real-time analysis of potentially malicious content in all vectors.
4. Email security requires real-time threat analysis that coordinates with web, mobile and other defenses.
5. Malware defenses need to monitor both inbound and outbound HTTP and HTTPS traffic to prevent infection and detect command and control (CnC) communications.
6. Data loss prevention (DLP) approaches must address encrypted communications, and better control both inbound and outbound content flow.




# Appendix A: The Seven Stages of Advanced Threats and Data Theft

## Stage 1: Reconnaissance

Hackers access credentials and research social media profiles to gain intelligence about people they're targeting. Their goal is to build highly personalized "lures" that are likely to be opened and acted upon.

## Stage 2: Lures

There are two types of lures: web lures and email lures.

Web lures prey on human curiosity. They are a common tactic of search engine optimization (SEO) poisoning, where hackers lure recipients who are searching for breaking news, celebrity gossip and other popular topics. Web lures are increasingly sent in broad, untargeted attacks via social media, where they are spread among friends in private social networks.

Email lures rely less on news, events and social media. Instead, they typically contain a notification a user might expect to receive: order notifications, ticket confirmations, delivery notices, test emails and tax return information are the top five examples. Such seemingly typical content allows email lures to bypass spam filters. Email lures are usually sent in highly targeted, low-volume attacks to specific individuals using intelligence gleaned from social media.

Because a good email defense starts with a great web defense, are you confident your current defenses can analyze social media to identify lures and protect users? Do your web and email security solutions share and correlate threat intelligence? Do they recognize that 92 percent of spam contains a potentially unsafe URL?

## Stage 3: Redirects

Users are usually directed to a survey, a rogue anti-virus (AV) offer or a fake web page where an exploit kit is waiting. Traditional redirects include SQL and iFrame injections that take users blindly down a path to services, content and offers they often do not desire. "Malvertising" (malware advertising) is a tactic to redirect unknowing users from within popular websites. Newer redirect tactics include postings made to social networking websites, fake plug-ins, fake certificates and heavily obfuscated JavaScript.

Redirects are often dynamic and change quickly — are your defenses fast enough to assess these web links in real time?

## Stage 4: Exploit Kits

In the past, hackers used lures to redirect users down a path that would enable malware to be installed onto their systems. It was a method that, though damaging at first, could be quickly detected by threat lab intelligence and thereafter prevented. Today, exploit kits such as Blackhole are used to deliver a malware dropper file, and this dropper file is sent only after a vulnerability is detected in a targeted system. If no vulnerability is detected, the user is redirected to a safe web page and the exploit kit remains hidden.

An understanding of exploit kits is important for analyzing advanced threats and developing real-time defenses. For example, Blackhole uses criminal encryption, which means that AV engines and generic deobfuscation tools will have difficulty detecting it.

Is AV your only defense at the web gateway? If so, it's highly likely that exploit kits can penetrate and infect your systems through vulnerable applications.

## Stage 5: Dropper Files

This stage is where most organizations focus their forward-facing defenses, which analyze every file entering their networks for malware. Unfortunately, what worked in the past might now provide a false sense of security. The problem is that few AV engines can detect today's dropper files that use dynamic packers for which no known signatures and patterns are available. One of the most popular dropper files is Rogue AV, which contains a fake offer to scan and clean your system. Traditionally focused on Windows systems, new versions such as Mac Defender or Protector are now targeting Apple computers.

What do you have other than AV to protect against advanced threats and data theft?

Note: The next two stages indicate two inescapable conclusions: No defense is 100 percent effective, and containment is the new defense for data loss prevention (DLP).



## Stage 6: Call Home

A typical advanced attack "calls home" to download malware and tools and send back valuable information. The problem is that most defenses are only forward-facing — they do not analyze the outbound call-home communications sent from within an infected system. And these call-home communications commonly use dynamic DNS to avoid detection.

Fortunately, there are emerging technologies to defend against this stage of advanced attacks. For example, infected systems and bots attempting to call home can be blocked from using dynamic DNS, while users can opt to continue on to trusted sites. Destination awareness in the context of DLP is also a potential defense, as is geo-location awareness. (In the latter case, however, because most malware communications, hosting and phishing originate in the United States, most policies will not block these domains.)

Do you have defenses that analyze outbound traffic for call-home communications? Can they perform contextual analysis of data, user, destination and other variables to prevent confidential information from being sent to personal web mail and social media accounts or saved on personal cloud storage accounts?

## Stage 7: Data Theft

Data, in the end, is what attackers are after. And data is what attackers get when they are able to bypass the insufficient security defenses at the previous six stages. Yet even at this seventh stage there are defenses emerging to keep confidential data safe.

Can your defenses detect password files leaving your network or the use of criminal encryption on outbound files? Can they catch confidential information being exported in low volumes per request (drips) to avoid detection over a defined period of time? Do they provide forensic reporting that shows what data was blocked from leaving your organization?

## Appendix B: Websense 2013 Security Predictions

2012 began with a report from IDC stating “Signature based tools (anti-virus, firewalls and intrusion prevention) are only effective against 30-50 percent of current security threats. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly.” Much of this can be attributed to how attacks evolved to specifically counter those defenses. To address this exposure, IDC recommended that organizations consider “a shift in security posture toward being more proactive.”

As 2012 came to a close, IDC’s recommendation still held true. A more proactive security posture requires advanced planning for the threats to come in the new year. To help you achieve this goal, we tapped our Websense® Security Labs™ researchers to predict the key threats you should prepare for in 2013.

After careful analysis of Websense ThreatSeeker® Intelligence Cloud data and other security intelligence and trends, they produced the following seven predictions you can use to review current defenses, identify security gaps and prepare new safeguards.

1. Attacks will continue to exploit legitimate web platforms. This includes hundreds of new content management systems and service platforms, in addition to the IIS and Apache exploits of the past.
2. More cross-platform threats will involve mobile devices. More than mobile-threat hype, there are specific emerging desktop, cloud and other technologies that will add to this growth.
3. Legitimate mobile app stores will host more malware. The success of mobile devices, the mobile app sales model and the pure volume of apps are creating a new area of risk.
4. Successful “hacktivism” incidents will decrease. Increased awareness, and the resulting improvements in defensive measures, will result in fewer successful hacktivism incidents, although attacks will increase in sophistication.
5. Government-sponsored attacks will increase. In the wake of several public cyberwarfare events, a number of contributing factors will drive more countries toward cyberwarfare strategies and tactics.
6. Threats will become more “virtual aware.” As network and security vendors apply virtual machines for applications, servers and sandboxing, cybercriminals will customize their threats accordingly.
7. Email threats will evolve to new levels. Domain generation algorithms and other emerging techniques bypass current security, and professionals are becoming the preferred targets. And malicious email attachments are making a comeback.

Overall, the sheer volume of attacks will continue to increase even while the average incident size declines. Based on customer feedback from private consultations, the full report also includes several Spotlight articles on the broader topics of mobile security, email security and Java exploits. This additional information may assist organizations in setting priorities and planning security projects in these key areas.

Download the full Websense 2013 Security Predictions report at www.websense.com\2013predictions.

# ABOUT WEBSENSE

Websense, Inc. (NASDAQ: WBSN), a global leader in unified web security, email security, mobile security and data loss prevention (DLP), delivers the best information security for advanced threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market and small organizations around the world. Distributed through a global network of channel partners and delivered as appliance-based software or SaaS-based cloud services, Websense® TRITON™ information security solutions help organizations use social media and cloud-based communication, while: protecting them from advanced attacks and modern malware; preventing the loss of confidential information; and enforcing Internet use and security policies.

The TRITON architecture is powered by Websense ACE (Advanced Classification Engine), which uses more than 10,000 advanced analytics and composite risk scoring to detect advanced malicious attacks that evade legacy security solutions. ACE analytics are derived from the Websense ThreatSeeker® Intelligence Cloud and maintained by Websense Security Labs.™ The ThreatSeeker Intelligence Cloud unites more than 900 million endpoints and, with the help of ACE, analyzes the content of up to five billion requests per day. To analyze malware and other threats, organizations can also utilize ThreatScope,™ a cloud-based malware analysis sandbox environment, to safely test potential threats.

Websense Security Labs drives security research and discovers, investigates and reports on advanced threats that traditional security research methods do not capture. Recognized as a world leader in security research, Websense Security Labs publishes findings to hundreds of security partners, vendors, media outlets, military and other organizations around the world 24 hours a day, seven days a week on the award-winning Websense Security Labs blog. With a team of more than 100 global threat experts and operations in the Americas, Europe, Middle East, Africa and Asia Pacific, Websense Security Labs continuously monitors threats that include Internet-borne threats, and those that stem from web, email, instant messaging and peer-to-peer file-sharing.

Websense is headquartered in San Diego, California with offices around the world.