

The Vertical Risk

Web-Delivered Malware Impact by Industry

ScanSafe STAT Analysis October 2008

EXECUTIVE SUMMARY

The type and frequency of Web-delivered malware changed dramatically in 2008. Chief among the causative factors was the marriage of profit-motivated attackers to automated tools that streamline both the discovery and the compromise of vulnerable websites. While SQL injection attacks have by far been the most prevalent attacks on websites throughout 2008, all forms of website compromise have been on the increase. These compromises are not occurring by the hundreds or even the thousands, but rather can be counted in the millions.

Each month, the ScanSafe Security Threat Alert Team (STAT) publishes the Global Threat Report which provides insight into the evolving Web threat landscape based on in-depth analysis of Web malware blocks performed on behalf of all ScanSafe customers. As noted in the September Global Threat Report, the volume of Web-delivered malware increased 338% in the third quarter of 2008 compared to 1Q08 and increased 553% compared to 4Q07.

To determine how this heightened risk translates to specific sectors of industry, ScanSafe STAT analyzed Web malware blocks specific to 21 industry verticals throughout the first three quarters of 2008: Agriculture & Mining, Aviation & Automotive, Banking & Finance, Charity & Non-Profit, Education, Energy & Oil (includes Utilities), Engineering & Construction (includes Heating & Plumbing), Food & Beverage, Government, Healthcare, Insurance, IT & Telecommunications, Legal & Accounting, Manufacturing, Media & Publishing, Professional Services, Pharmaceutical & Chemical, Transportation & Shipping, Travel & Leisure, Real Estate, and Wholesale & Retail.

This analysis was initially undertaken to address the question: Do certain industry verticals encounter more Web-delivered malware than others? The initial results were startling. Not only did it appear that certain industry verticals encountered more Web-delivered malware than others, but those verticals with the highest incidents of Web malware encounters were Energy & Oil, Pharmaceutical & Chemical, Engineering & Construction, Transportation & Shipping, and the Travel industry.

This ScanSafe STAT Vertical Risk Assessment presents the results of that analysis, detailing the vertical rates of exposure to Web-delivered malware as well as providing an analysis of the types and severity of the malware encountered.

Methodology

ScanSafe is the pioneer in the Web SaaS arena, providing true in-the-cloud, real time, parallelized processing and scanning of both incoming and outgoing Web requests. This unique perspective enables ScanSafe to intercept, analyze, and defend against Web threats as they occur. Aside from the obvious advantages that real-time Web traffic scanning provides from the standpoint of prevention, real-time scanning also enables far more accurate assessment of the actual level of risk confronted in today's enterprise. As an example, Web crawling technologies can provide some insight into the numbers of websites hosting malware, but no insight into whether those sites are being accessed, i.e. the actual risk of encounter. Cloaking and other technologies can also result in misinterpretation of findings. Conversely, ScanSafe's real-time Web traffic assessment reflects actual user experience and thus removes the bias associated with more speculative analyses.

The reporting period covers the first three quarters of 2008, from January 1 through September 30, 2008. During this reporting period, on average, ScanSafe processed 17 billion Web requests per month, performing approximately 170 million blocks per month on behalf of all ScanSafe customers¹.

Web threats discussed in this report are those related only to 'worst category' malware threats: actual worms, viruses, Trojans (including keyloggers, password stealers, and non-consensual spyware), exploit code or the associated malicious iframes or malicious source references used to load the aforementioned malware. Malicious forms of spyware are included, but blocks resulting from adware, tracking cookies, and Web bugs are excluded. Unless otherwise specified, Web block statistics provided in the ScanSafe STAT Vertical Risk Assessment are based on the point at which the block occurred. This method results in an under-representation of actual malware binaries resulting from compromised websites. The June and August 2008 editions of the ScanSafe Global Threat Report include the most recent data analysis of intended malware resulting from compromised websites.

To ensure equal representation across all verticals, the weight of each respective vertical was calculated based on the number of customers within the specific vertical in comparison to the total number of all customers across all verticals:

Weight = Customers in Vertical / Customers in All Verticals
Normalized = Blocks per Vertical / Weight

The normalized value was then compared to the median for all blocks across the verticals, for each of the respective categories analyzed. A positive value reflects a higher than median rate of encounter; a negative value reflects a lower than median rate of encounter; zero reflects a median rate of encounter. No adjustment was made based on number of employees at individual companies. Web surfing habits may vary considerably among employees; the intent of this analysis was to determine the comparative rates of encounters for each vertical as opposed to encounters by user. Analysis is based solely on Web malware block data for which vertical correlation was available. The results of this analysis and any conclusions drawn from those results should be considered applicable to Web malware events only and may not be consistent with all Web surfing experiences.

¹ On average for the reporting period specified. Currently ScanSafe processes 20 billion requests per month with 200 million blocks resulting.

Key Highlights:

- The volume of Web-delivered malware is increasing at a rate of approximately 6% per month, but the rate of exposure to that malware is increasing at a rate of approximately 16% per month.
- The Energy & Oil industry had a 156% higher encounter rate compared to the median of all Web malware encounters across verticals. Pharmaceutical & Chemical had the second highest encounter rate, at +152% of the median. Other verticals in the top 5 include Engineering & Construction (116%), Transportation & Shipping (96%), and Travel & Leisure at +44% of the median.
- 28% of all Web malware blocks specific to the Pharmaceutical & Chemicals sector were for zero-day malware encounters. Engineering & Construction had the second highest rate of zero-day malware encounters at 21%, followed by Aviation & Automotive at 20%. The average rate of zero-day malware exposure across all verticals was 14%. The average rate for all ScanSafe customers is 18%.
- Among third party applications, exploits of vulnerabilities in Adobe Flash (SWF) and Adobe Reader (PDF) were the most commonly encountered, representing 83% and 13% of all detected third party application exploits respectively. Apple Quicktime was third at 3% followed by Microsoft PowerPoint at less than 1%.
- At +135% of the median rate, Transportation & Shipping had the highest rate of encounter with compromised websites, followed by Pharmaceutical & Chemical at 103%.
- Banking & Finance had the highest rate of exposure to Web-delivered Flash exploits at a rate of 3% of all Web-based malware blocks (or 23% of all blocks related specifically to third party application exploits).
- With a +1138% variance, exposure to backdoors and password stealers was exceptionally higher in the Pharmaceutical & Chemicals sector. Energy & Oil was second highest with a +342% variance, followed by IT & Telecommunications at 262%.
- Energy & Oil companies encountered unique variants of password stealers and backdoors at a much higher rate compared to other verticals. During the reporting period, Energy & Oil encountered 213 unique variants of this class of malware, compared to the average of 58 unique variants for all verticals. Note that this is a count of unique variants encountered and not a count of the volume of variants encountered.

The Vertical Risk

The risk of Web-delivered malware encounters can be measured both in terms of volume of overall Web malware blocks compared to all Web requests, as well as changes in the levels of exposure among a specific group. For the latter measure, ScanSafe analyzes block data from a representative group of customers that are common to all reporting periods commencing with May 2007 onward. Based on the two measures, the volume of Web-based malware compared to all Web requests is increasing at a rate of approximately 6% per month and the current rate of exposure to that Web-encountered malware is increasing at a rate of approximately 16% per month. The faster growth of exposure vs. volume is believed to be a result of continually increasing numbers of website compromises.² These growth rates are provided for perspective purposes and may not apply specifically to the respective industry verticals included in this report.

To better understand how the risk of exposure plays out across industries, ScanSafe STAT analyzed Web malware blocks specific to 21 industry verticals throughout the first three quarters of 2008: Agriculture & Mining, Aviation & Automotive, Banking & Finance, Charity & Non-Profit, Education, Energy & Oil (includes Utilities), Engineering & Construction (includes Heating & Plumbing), Food & Beverage, Government, Healthcare, Insurance, IT & Telecommunications, Legal & Accounting, Manufacturing, Media & Publishing, Professional Services, Pharmaceutical & Chemical, Transportation & Shipping, Travel & Leisure, Real Estate, and Wholesale & Retail. Block data was normalized to adjust for differences in the number of companies representing each vertical. The breakdown of representation in the industry verticals is shown in Figure 1 below.

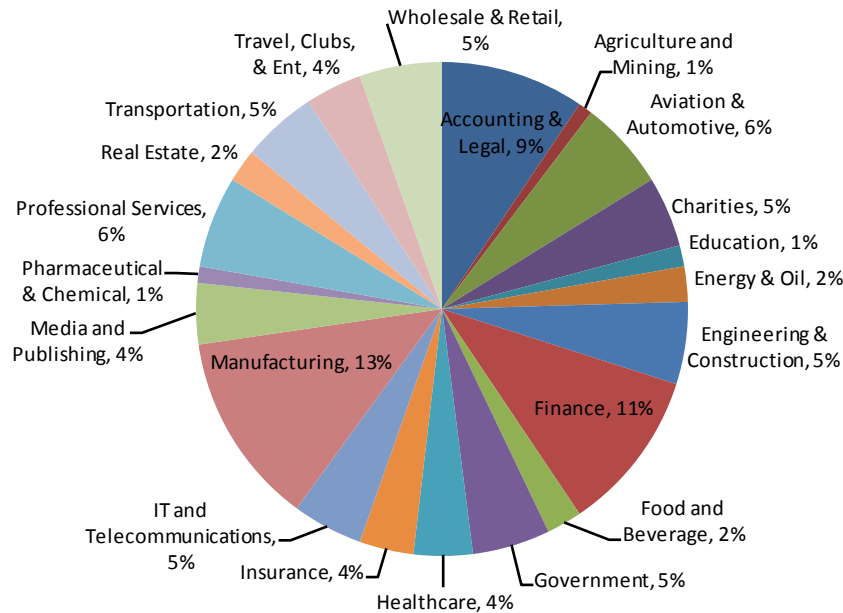


Figure 1

For comparison purposes, Figure 2 shows the breakdown across categories of the collective Web malware blocks for all verticals included in the study.

² Growth rates are provided for perspective purposes and may not apply specifically to the respective industry verticals included in this report.

Combined Malware Blocks - All Verticals

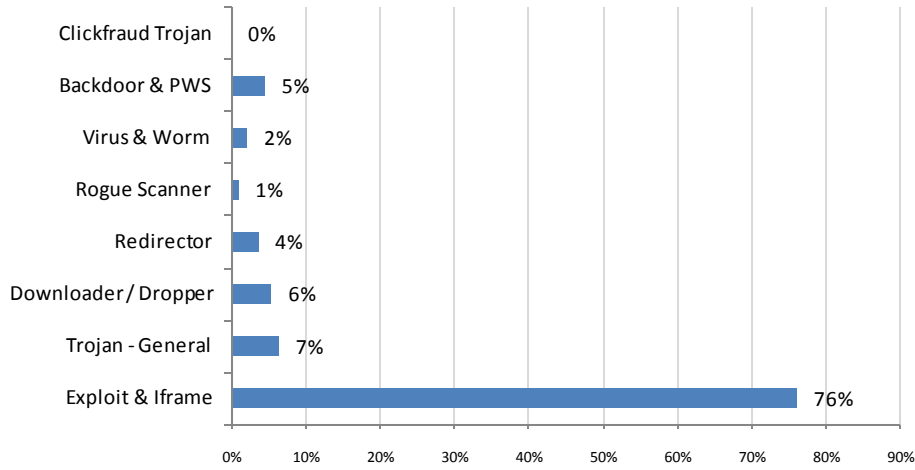


Figure 2

Figure 3 reflects the variance between the median of Web malware blocks per vertical. Higher percents reflect higher numbers of Web-delivered malware encounters.

Percent Variance of All Blocks by Vertical

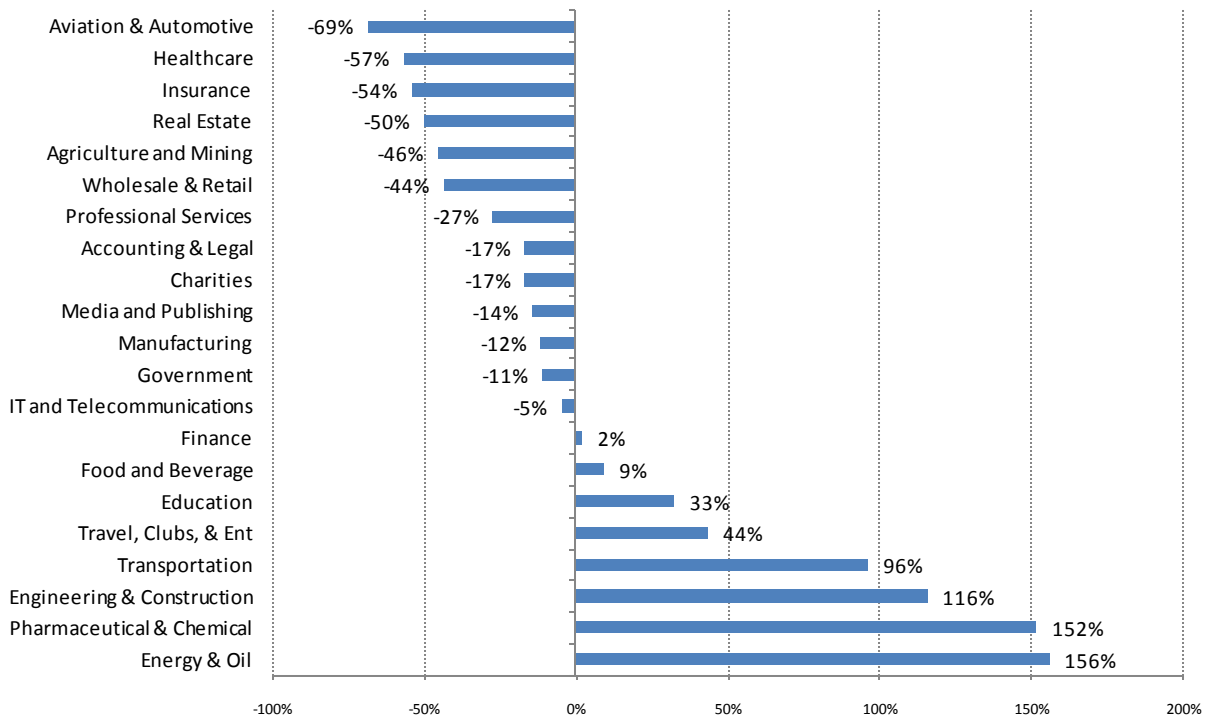


Figure 3

An important disclaimer is needed here. This research is not intended to be commentary on cybercrime or terrorism, nor is it intended as a reflection on potential impact to global economies or potential insecurities of any

given industry. It is, however, intended to demonstrate not only the severity of the Web-delivered malware threat, but specifically the risk that Web-delivered malware poses to the enterprise.

Malware blocks are reported based on the stage at which the block occurred. The majority of blocks result from compromised websites, specifically the malicious iframe or malicious source reference implanted on the compromised site. A block may also be triggered on an attempt to launch exploit code resulting from the malicious iframe or malicious source reference. Collectively, this category of blocks is referred to as “iframes and exploits” and is the largest category of ScanSafe Web malware blocks. A Web surfer may also encounter a malware binary directly, i.e. that encounter is not preceded by a blocked conduit such as a compromised website but instead results from some other delivery exposure, such as following a link in a socially engineered email. While the ScanSafe service doesn’t process email specifically, malicious traffic resulting from links contained within the email will be detected.

User-initiated actions can play a key role in supporting or undermining an organization’s security posture. While it is impossible to judge intent, it is possible to glean some insight into whether an encounter resulted accidentally (i.e. via a conduit such as a compromised website) or whether it occurred as a result of some more deliberate action, (i.e. clicking a link in email). Additionally, some events that appear to be user-initiated may be the result of internal infection or other internal cause.

Though there is no direct way to measure intent based solely on Web traffic, we can examine referrer traffic (or rather the lack thereof) to determine if a particular encounter might have been user-initiated or otherwise the result of direct internal action. And while the lack of referrer isn’t evidence in and of itself, when viewed from the standpoint of possible user-initiated actions or pre-existing infections, it does become an interesting data point to consider. Figure 4 reflects the variances in occurrence of non-referrer Web traffic amongst the various verticals.

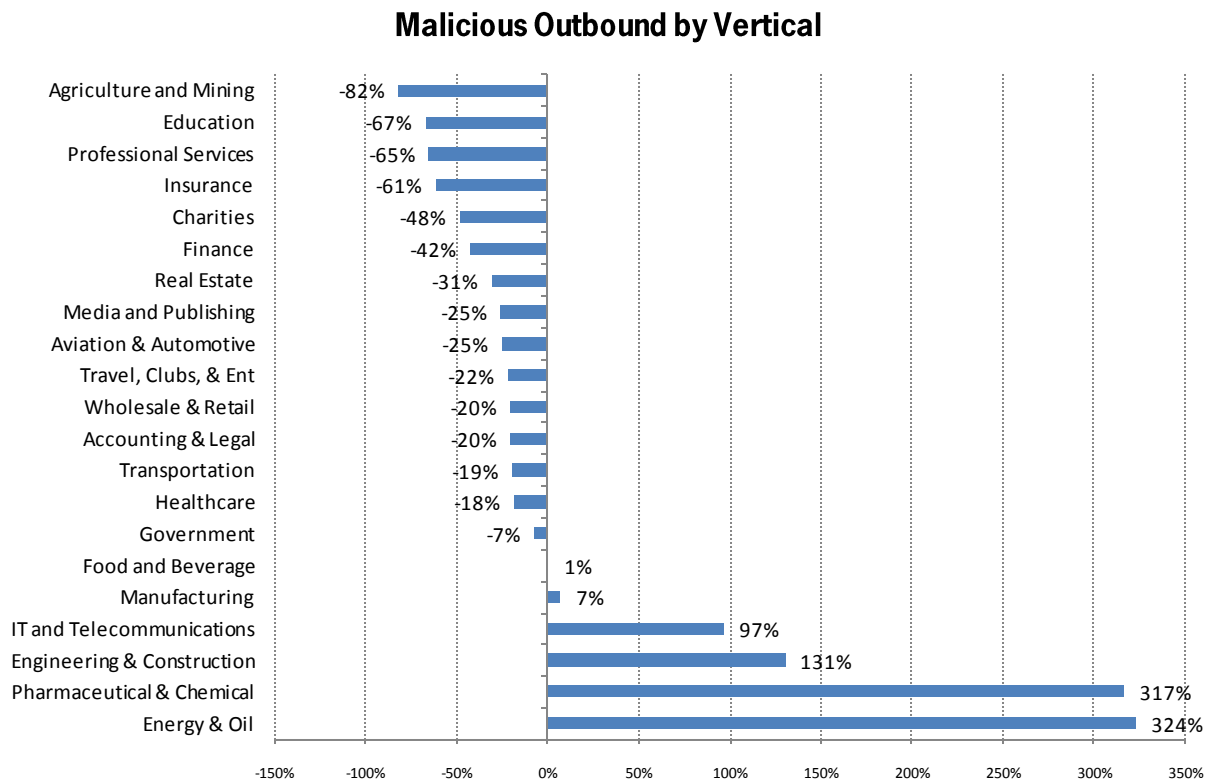


Figure 4

Encounters with Compromised Websites

The majority of encounters across all verticals were encounters with malicious iframes and malicious source references implanted on compromised websites. These iframes and source references automatically load external content from attacker owned sites. Generally, that external content consists of exploit code that targets various vulnerabilities within the operating system, browser, or third party applications in an attempt to install malicious binaries such as Trojan downloaders, backdoors, and password stealers. This exploit code and the resulting malware are launched silently. Unlike the so-called drive-by downloads circa 2004, today's forcible Web installs are performed quietly and surreptitiously. The compromised site continues to look and function normally and the visitor's experience is generally not disrupted by the silent malware installation.

The vertical variance in encounters of malicious iframes, malicious source reference, and exploit code can be seen in Figure 5.

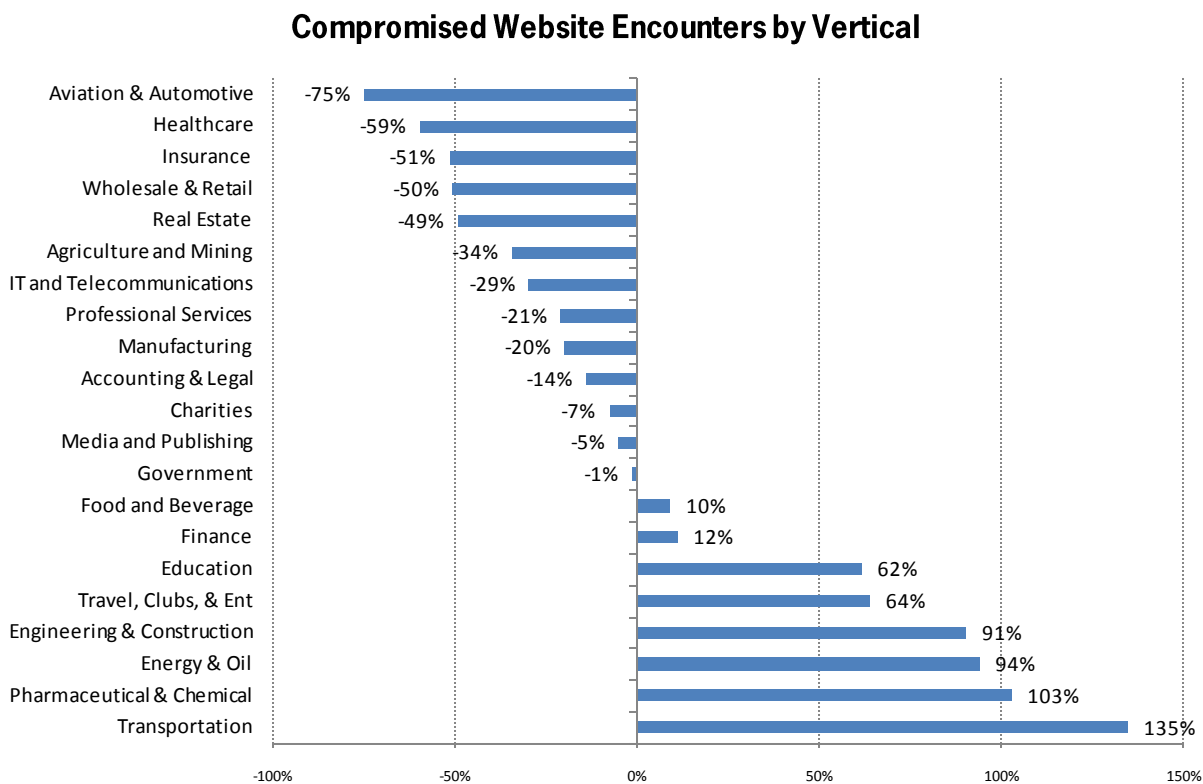


Figure 5

Among third party applications, exploits of vulnerabilities in Adobe Flash (SWF) and Adobe Reader (PDF) were the most common, representing 83% and 13% of all detected third party application exploits respectively. Apple Quicktime was third at 3% followed by Microsoft PowerPoint at less than 1%. Flash, PDF, and Quicktime exploits are common deliverables resulting from compromised websites, thus it is not unexpected that these represent 99% of third party application exploits blocked by ScanSafe on behalf of customers represented in the vertical assessment.

Banking & Finance had the highest rate of exposure to Web-delivered Flash exploits at a rate of 3% of all Web-based malware blocks (or 23% of all blocks related specifically to third party application exploits). Banking & Finance and Manufacturing both had the highest rate of exposure to Web-delivered PDF exploits, at a rate of 0.2% each for all Web-based malware blocks.

Encounters involving malformed PowerPoint documents were extremely rare (approximately 0.12%), with those encounters resulting from webmail exposure only.

Among malformed image files, malicious GIF files were the most commonly encountered (64%), followed by malformed JPG at 35%, PNG at 1% and BMP and TIFF at less than 1% collectively. Collectively, malformed image files represented 6% of all Web malware encounters of verticals included in the assessment.

Backdoors and Password Stealers

Malware purposed for data theft presents a significant security challenge for corporations. The stereotypical thinking of password stealers is malware engaged in credit card fraud or the theft of gaming credentials. In reality, much of today's Web-delivered password stealers are custom configurable and can be remotely programmatically customized to steal whatever data the attacker finds attractive. Backdoors provide the necessary communication configuration channel to enable the attacker to assess the victim and deliver the customized configuration to the installed password stealer.

With a +1138% variance, exposure to backdoors and password stealers was exceptionally higher in the Pharmaceutical & Chemicals sector. Energy & Oil was second highest with a +342% variance, followed by IT & Telecommunications at 262%.

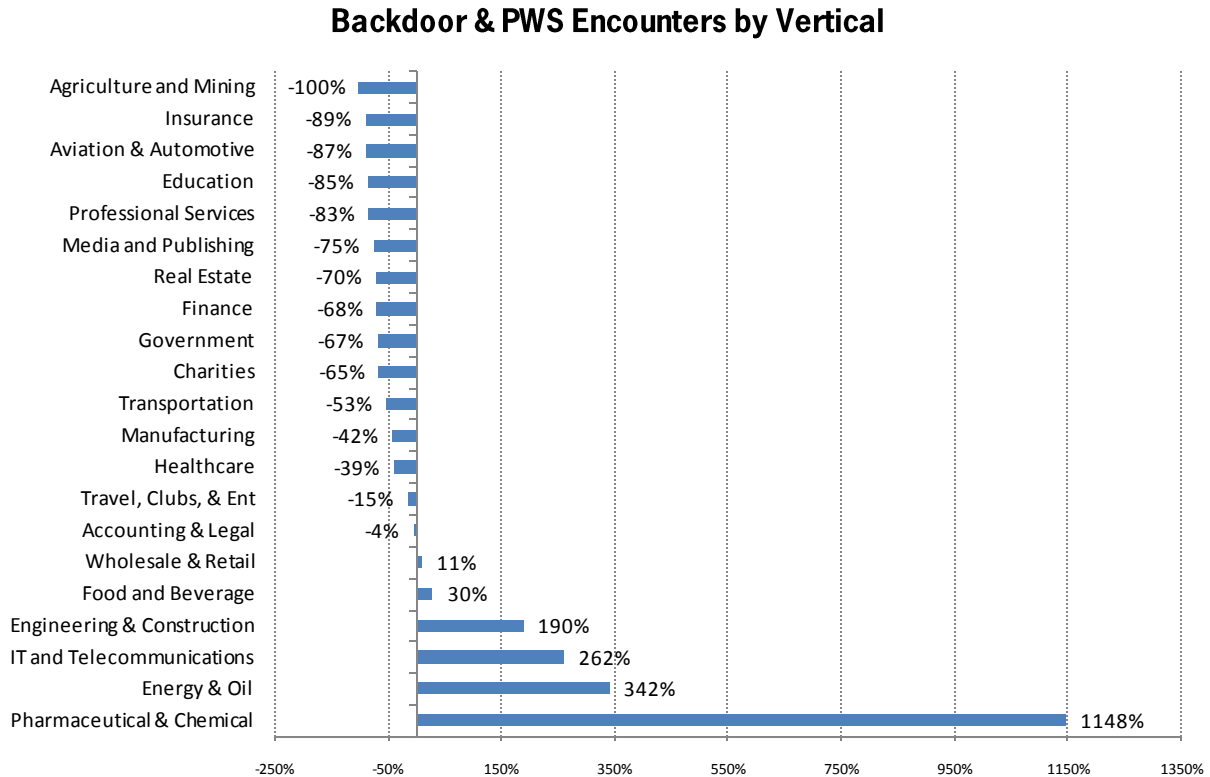


Figure 6

In total, 859 unique variants of password stealers and backdoors were blocked during the first three quarters of 2008. This is not the total number of backdoors and password stealers blocked, but rather a count of the number of individual variants that were encountered. The following chart is not normalized and depicts the total count of unique variants per vertical.

Unique Backdoor/PWS Variant Count

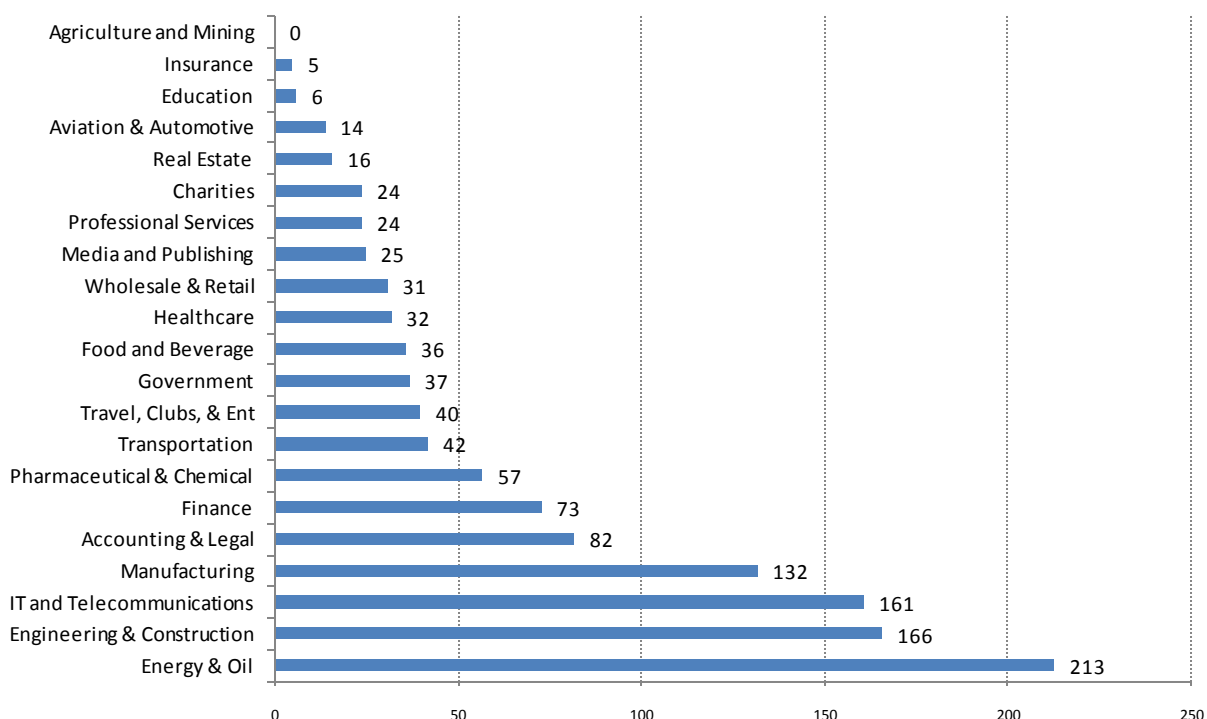


Figure 7

Win32.Agent.knt	8%
Win32.Bifrose.yzr	6%
Win32.Zlob.jbe	3%
Win32.Poison.dzd	3%
Win32.OnLineGames.yzt	3%
Win32.OnLineGames.uir	3%
Win32.Small.flb	2%
Win32.Poison.djv	2%
Win32.OnLineGames.w hs	2%
Win32.OnLineGames.siy n	2%

At 8% of encounters to backdoors and password stealers, Win32.Agent.knt was the most frequently encountered malware in this category. This Trojan was also encountered by the highest number of verticals (19 of the 21).

The ScanSafe STAT Vertical Risk Assessment reports malware blocks only at the stage in which the block occurred. The majority of blocks (76%) were blocks which occurred prior to actual exposure to the malicious binary. Previous analysis indicates that the preponderance of non-Asprox website compromises attempt to download backdoors and password stealers, while Asprox-related compromises typically attempt to download a category of malware referred to as rogue scanners, a term which sounds deceptively benign.

Rogue scanners may act as Trojan downloaders, may include backdoor functionality, and may result in fraudulent credit card charges for victims. Non-Asprox attacks were the most common method of website compromise in the

first half of the year, whereas Asprox-related attacks have been the dominant force in website compromises from June 2008 onwards.

Rogue scanner blocks represent only 1% of all malware blocks performed on behalf of customers included in the vertical industry assessment, though once again this number is under-reported since most malware blocks occurred at the point of access to the compromised site, prior to actual binary exposure.

Downloaders and Droppers

Downloader and dropper Trojans have an unpredictable impact on organizations. The intended binaries can be changed at the whim of the attacker, thus the functionality and severity of the attack may vary considerably. This uncertainty leads to unique challenges as it can often be difficult for administrators to determine what malware may have subsequently been installed as a result of the original infection.

Based on total volume of blocked downloaders and droppers blocked, the most frequently encountered variant was a variant of Win32.Dadobra.adk – a downloader that could be classified as a password stealer as it also includes keylogging capabilities.

The following chart provides the variance of exposure to downloader and dropper Trojans amongst the analyzed verticals.

Win32.Dadobra.adk	4%
Win32.Delf.hdu	4%
Win32.Agent.vyi	3%
SWF.Gida.a	3%
Win32.Exchanger.fd	3%
Java.OpenConnection.ao	3%
Win32.Agent.qpv	3%
Java.OpenStream.c	2%
Java.OpenConnection.aj	2%
SWF.Small.u	2%

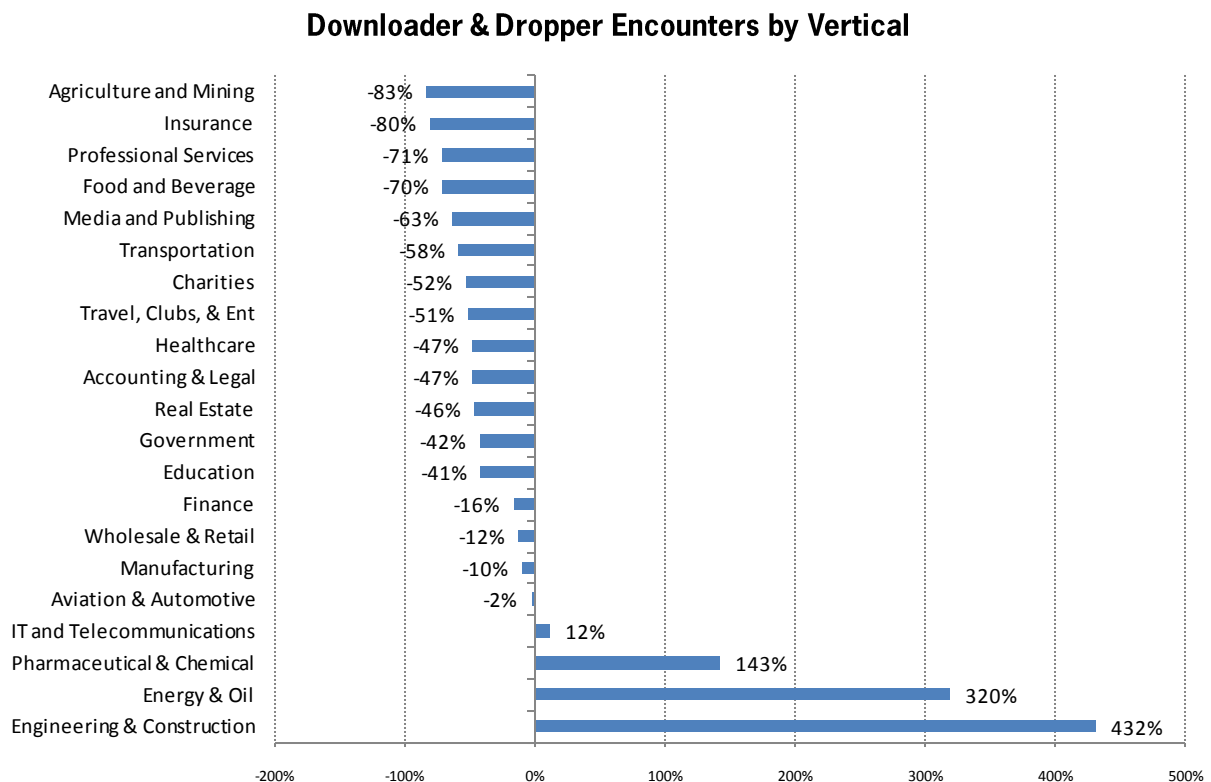


Figure 8

751 unique variants of downloader and droppers were blocked by ScanSafe on behalf of the verticals during the first three quarters of 2008. The unique variant count is not a count of actual numbers of downloaders and droppers blocked, but rather a count of the number of different variants encountered. The following chart is not normalized and depicts the total count of unique variants per vertical.

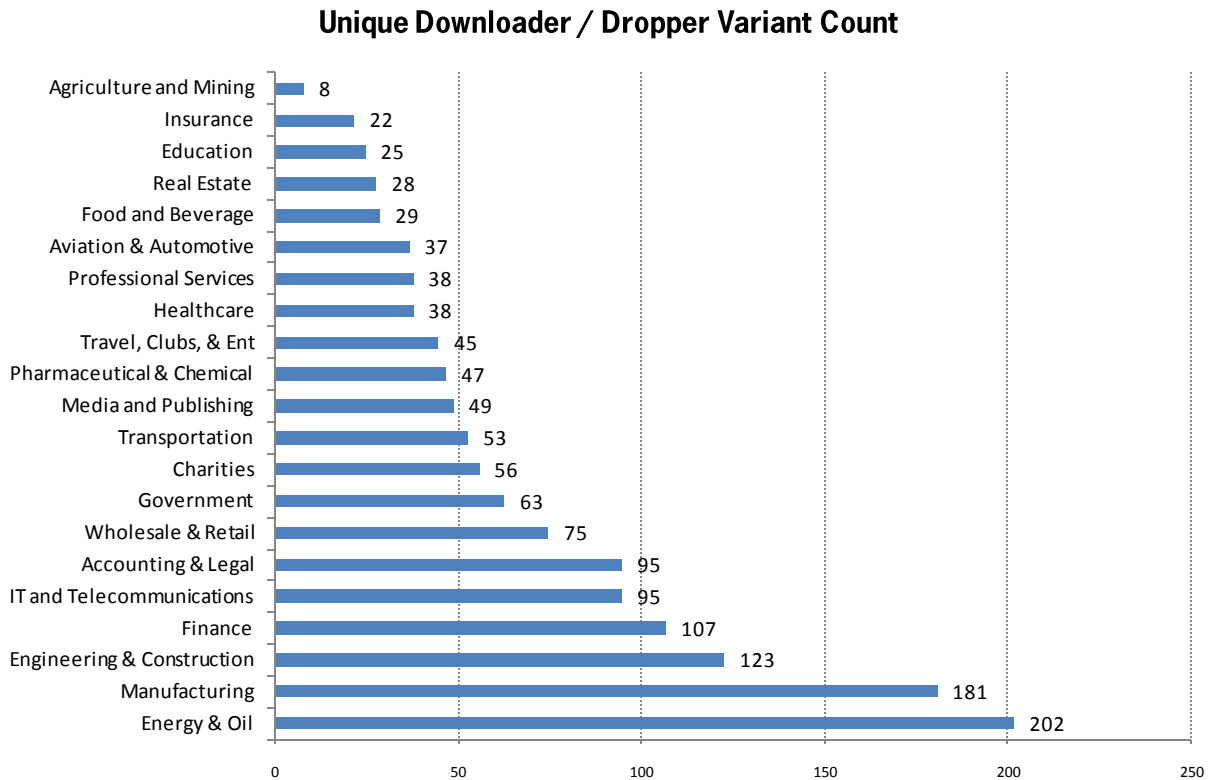


Figure 9

Zero-Day Malware Threats

ScanSafe defines zero-day malware threats as verified malware blocks which occur as a result of ScanSafe’s layered Outbreak Intelligence (OI) technologies and which were not detectable by signature-based technologies at the time of encounter. During the first three quarters of 2008, the average rate of zero-day malware was 18% for all customers. For customers included in the ScanSafe STAT Vertical Threat Assessment, the average rate of zero-day malware for all verticals combined was 14%.

Zero-day malware percentages are calculated individually for each vertical, thus the rate provided is indicative of the rate of zero-day detection compared to the overall number of Web malware blocks for that respective vertical only. At 28%, the Pharmaceutical & Chemicals sector had the highest rate of encounter to zero-day malware delivered via the Web. Engineering & Construction had the second highest rate of zero-day malware encounters at 21%, followed by Aviation & Automotive at 20%. Despite the Aviation & Automotive industry’s higher ratio of zero-day malware encounters, that sector had the lowest rate of exposure to Web-based malware overall.

The Energy & Oil industry had an average rate of encounter (among verticals) to zero-day Web-based malware, at 14%, still below the all customer average of 18%. Education and Agriculture & Mining sectors had the lowest rate of zero-day malware exposure via the Web, at 3% and 2% respectively.

Percent Zero-Day Malware Per Vertical

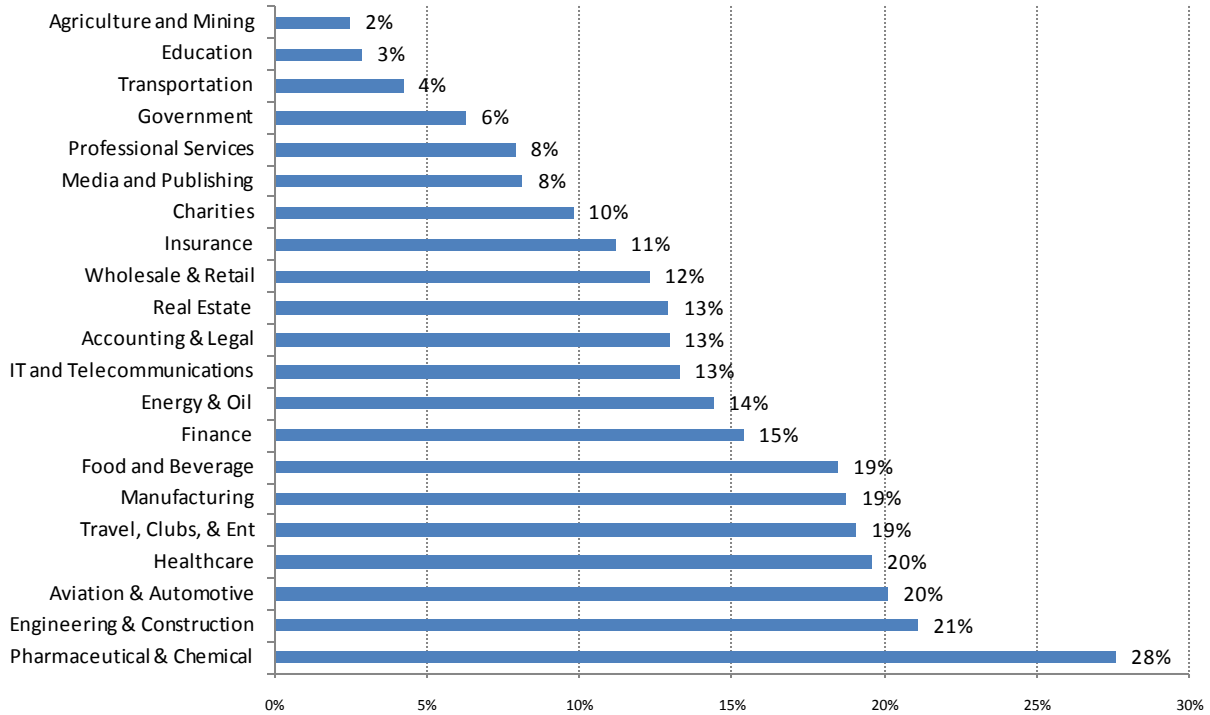


Figure 10

Top 5 Verticals

The following charts provide Web malware block data specific to each of the top five verticals based on volume of Web malware encounters within the respective vertical.

Malware Block Category % Per Vertical

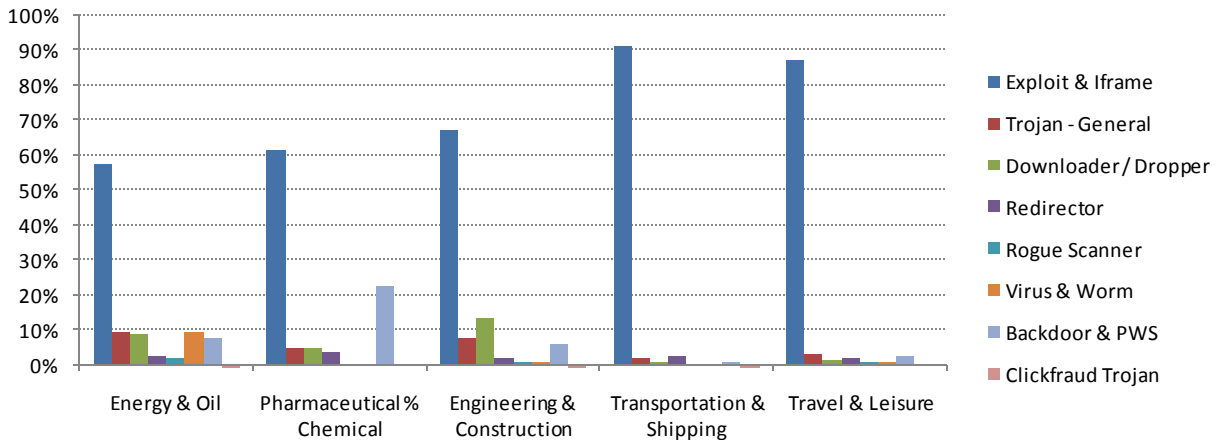


Figure 11

The final chart is a three dimensional view of the block variance from median for each of the verticals shown for each category of malware block.

3D View of All Blocks Variance by Vertical

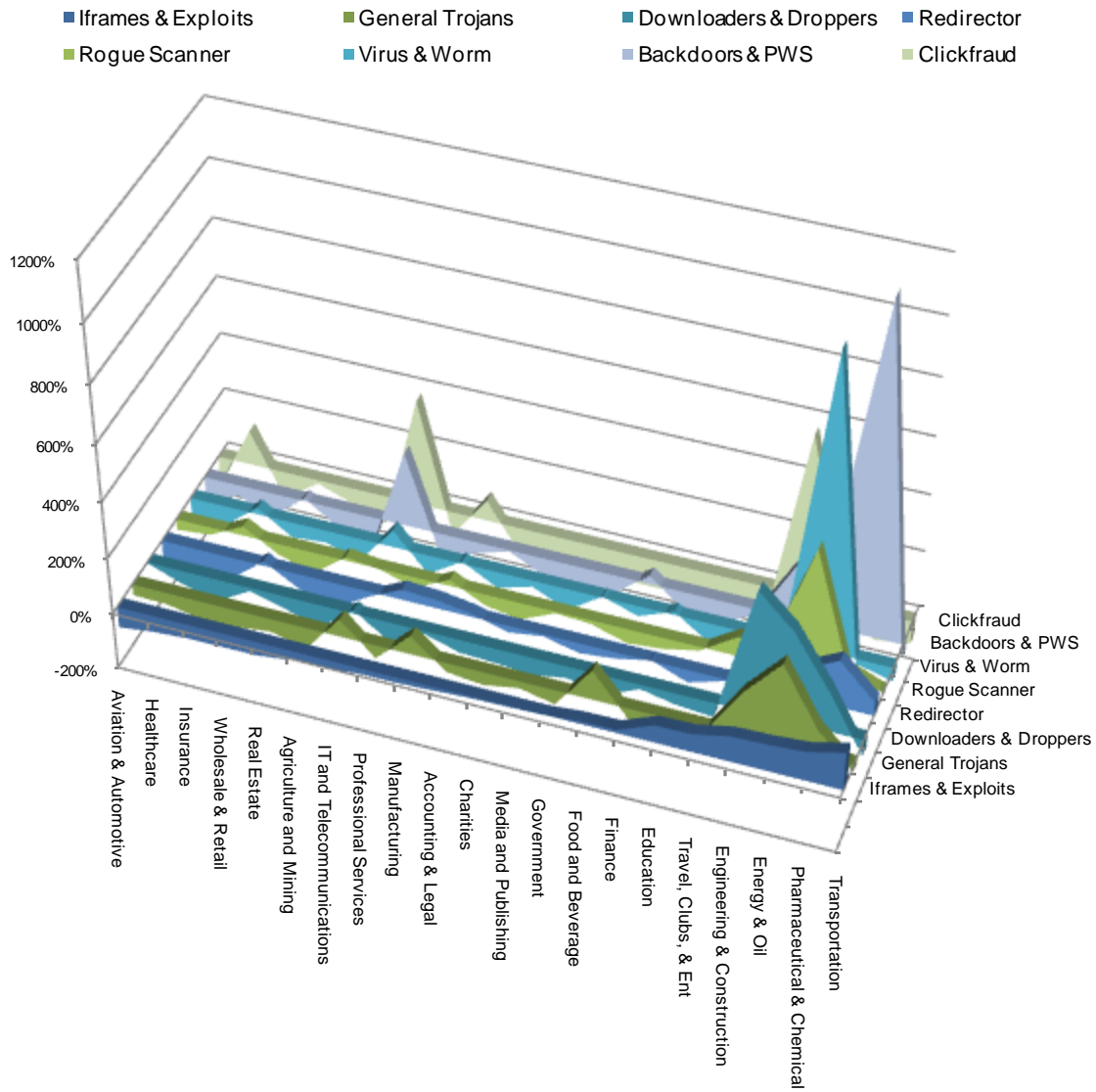


Figure 12

SUMMARY

The intent of this report is to simply provide a way to look at available vertical block data from various angles, perhaps providing the ability to spot trends or form assumptions. But when forming assumptions, it is important to understand the data doesn't in and of itself address the question of why. Indeed, quite often viewing the data from a pure numbers standpoint raises more questions than it attempts to address.

This project was undertaken to answer the question "do some verticals encounter Web-based malware at a higher rate than others". While the short answer certainly seems to be yes, the analysis raises plenty of other questions. Why do Energy & Oil, Pharmaceuticals & Chemicals, and Engineering & Construction have such considerably higher risk compared to other industry verticals? Why are these same verticals encountering backdoors and password stealers at a higher rate? Why are these same verticals encountering a higher number of unique variants of backdoors, password stealers, and downloaders compared to other verticals? What are the implications of the higher than average rate of user-initiated or internal outbound actions leading to Web malware exposure among the higher encounter verticals? The answers to these questions are beyond the scope and intent of this analysis but certainly they are questions deserving of an answer.

While wishing to avoid broad conjecture, observing the data from multiple viewpoints with astoundingly similar results does cause some pause. The industries consistently encountering the highest rate of Web-delivered malware are not ordinary industries, but rather industries that can have critical bearing on infrastructure and intellectual property rights.

We entered this analysis with the broad assumption that Web malware exposure was likely related to user surfing habits. With that expectation in mind, we fully expected to see verticals such as Travel in the top 5. After all, it seemed to us that employees in the Travel industry would be more likely to have a need to browse multiple diverse sites and thus have an overall higher exposure posture. This anticipated result did not pan out. Although Travel was a top 5 at-risk vertical, had our assumption been valid we would have anticipated certain other verticals to move to the forefront of exposure risk. For example, Media & Publishing or Education would have been our imagined contenders given the heavy amounts of online research one would anticipate in those particular verticals. Instead, we were surprised with Energy & Oil, Pharmaceuticals & Chemicals, Engineering & Construction and Transportation & Shipping.

The analysis contained in this report is based on Web malware block data only. Statistical risk assessment would require an assessment of the volume of Web malware blocks compared to all Web requests for each vertical. This level of analysis was beyond the scope of this report. The only conclusion that can be drawn is that when Web malware encounters do occur, the rate of encounter is higher among very sensitive verticals.

11.0 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.

Contact ScanSafe

ScanSafe US
185 Berry Street
San Francisco, CA 94107
T: 415 692 2000
F: 415 536 5949
E: 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

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