

The Global Malware Problem: Complacency Can Be Costly

An Osterman Research White Paper

Published June 2011

SPONSORED BY



Osterman Research, Inc.

P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

The Global Malware Problem: Complacency Can Be Costly

Today, malware is a given on the Internet. With tens of thousands of malware variants discovered every day, organizations of all sizes experience enormous financial losses as cybercriminals steal financial and customer data. Plus, IT labor costs continue to increase as IT staff members scramble to remediate malware infections, and user productivity suffers due to malware-induced outages.

Complicating the problem, not enough decision makers and other corporate influencers address malware threats adequately. Instead, they face factors such as budget constraints, unawareness of the severity of current and future malware threats, and a tendency to address these problems reactively, rather than proactively. This all leads to a type of complacency, which is underscored by the fact that while 49% of survey respondents acknowledge that security breaches occur; they simply accept this as part of the cost of doing business. However, the costs are typically higher than many organizations realize, but with the right knowledge and technologies, it is possible to reduce the impacts of malware.

SURVEY BACKGROUND AND METHODOLOGY

In May 2011, Osterman Research conducted a large, in-depth survey to understand how serious the malware problem is in real-world environments.

- 92% of the respondents were decision makers and influencers in their organizations' IT departments.
- The 17-question survey was conducted online and included members of the Osterman Research survey panel.
- Small, mid-sized, and large organizations were included in the survey, with a mean number of 10,676 employees across a wide range of industries (with a skew toward the education vertical).

KEY TAKEAWAYS

- Many decision makers and influencers believe they have little or nothing to worry about in the context of breaches or network downtime, despite the fact that most organizations have experienced malware attacks.
- For example, during the past 12 months, 70% of organizations have experienced a Web-borne malware infection and 50% have experienced malware infiltration through email.
- Moreover, 70% of organizations indicate that a typical attack on their organization would carry with it a serious financial impact – 25% estimate that a single attack would cost their organization more than \$10,000.
- One in six attacks result in a regulatory violation, which by itself could cost an organization millions of dollars.

- Nearly 75% of organizations believe that smartphones and tablets are becoming a significant security concern, but many lack security solutions focused on these platforms.
- The consequences of malware can range from merely annoying, which require IT staff time to remediate, to catastrophic, resulting in the loss of hundreds of thousands or millions of dollars.
- Organizations must take a proactive approach to detecting and remediating malware to address both tactical and strategic requirements.

ABOUT THIS WHITE PAPER

This white paper discusses the survey results as well as today's critical malware problem, the direct and indirect costs to organizations, and the hurdles faced in preventing these threats.

Overconfident and Underprepared

There is a natural human tendency toward reactivity—to remediate problems aggressively after they have occurred, but to dismiss or postpone addressing risks in a proactive manner. In the context of malware and other security threats, a lack of proactivity is not so much the result of carelessness or inattention, but is driven by limited IT budgets, underestimation of the risks, or the inability to persuade senior management that these risks are serious and worthy of action.

MANY NEED TO IMPROVE THEIR SECURITY

Despite the relatively high level of confidence in many organizations' current application and network security capabilities, there are some issues over which decision makers and influencers have concerns:

- 53% agree or strongly agree that they need to manage and control Web 2.0 applications and social media better.
- 34% agree or strongly agree with the idea that social media has many legitimate business purposes, but they are afraid to open up access to their employees.
- 71% agree or strongly agree that smartphones and tablet devices are becoming a more serious security issue for their organization.

MOST ORGANIZATIONS VERY CONCERNED ABOUT MALWARE

It is also interesting to note that even with the high level of confidence in the application and network security infrastructure deployed at organizations that responded to our survey, there is still a significant level of concern about malware infiltration and data leakage from various sources:

- 77% are extremely concerned about malware entering their organization from the Web.
- 64% are extremely concerned about leakage of internal data from company employees.

- 66% are extremely concerned about malware entering their network through email.
- 42% are this concerned about a security breach impacting their corporate website.

LITTLE OR NOTHING TO WORRY ABOUT? THE PREVAILING MYTH

Despite the high level of concern about security issues, our research found that a large proportion of decision makers and influencers agree with the notion that their current security solutions are sufficient and that their organization does not need to worry about network breaches or downtime. Thirty percent of those surveyed responded that they are in general or strong agreement with this. Further, 59% of those surveyed feel that their risk is lower, on average, than other organizations that are similar to them; while 53% believe that their network security is better, on average, than other organizations.

Moreover, despite the high level of concern expressed about the security of mobile devices like smartphones, remote laptops and tablets, 14% of those surveyed have no solutions in place to protect users from Web-based threats. Even among those that do, the solutions are largely reliant on traditional anti-virus software installed on the devices; not solutions that will prevent data leaks or mitigate the threats from Web-based malware. For example, while 97% of respondents indicated that their organization has deployed some sort of anti-virus solution on laptops, only 60% have a secure Web gateway that is accessed via a VPN. Only 27% use data loss prevention tools on laptops, and 17% use a cloud-based Web security service. Furthermore, only 58% of organizations have anti-virus and provide a secure Web gateway for mobile users.

THE COMPLACENCY DISCONNECT

What this data tells us is that there is a significant disconnect between the concerns that organizations have about a) specific types of threats that could impact their organization, b) their high level concerns about network and application security, and c) what they are doing to improve their overall security posture.

What Are the Direct and Indirect Costs of Malware?

At its core, malware is nothing more than a tool to steal money and other valuable assets. Those who hold these assets are the hosts, and criminal organizations are the parasites that feed from these funds and content. A natural equilibrium is being established in the malware industry: cybercriminals want the host to stay in business so that they can continue to bleed them of funds and data for long periods. However, some rogue criminals do not appreciate this “macro” view of their industry and instead focus on targeting their potential victims heavily for short-term gain. The result, in Osterman Research’s opinion, will be continued escalation of malware, both in its stealth and in the severity of the impacts it creates for all organizations.

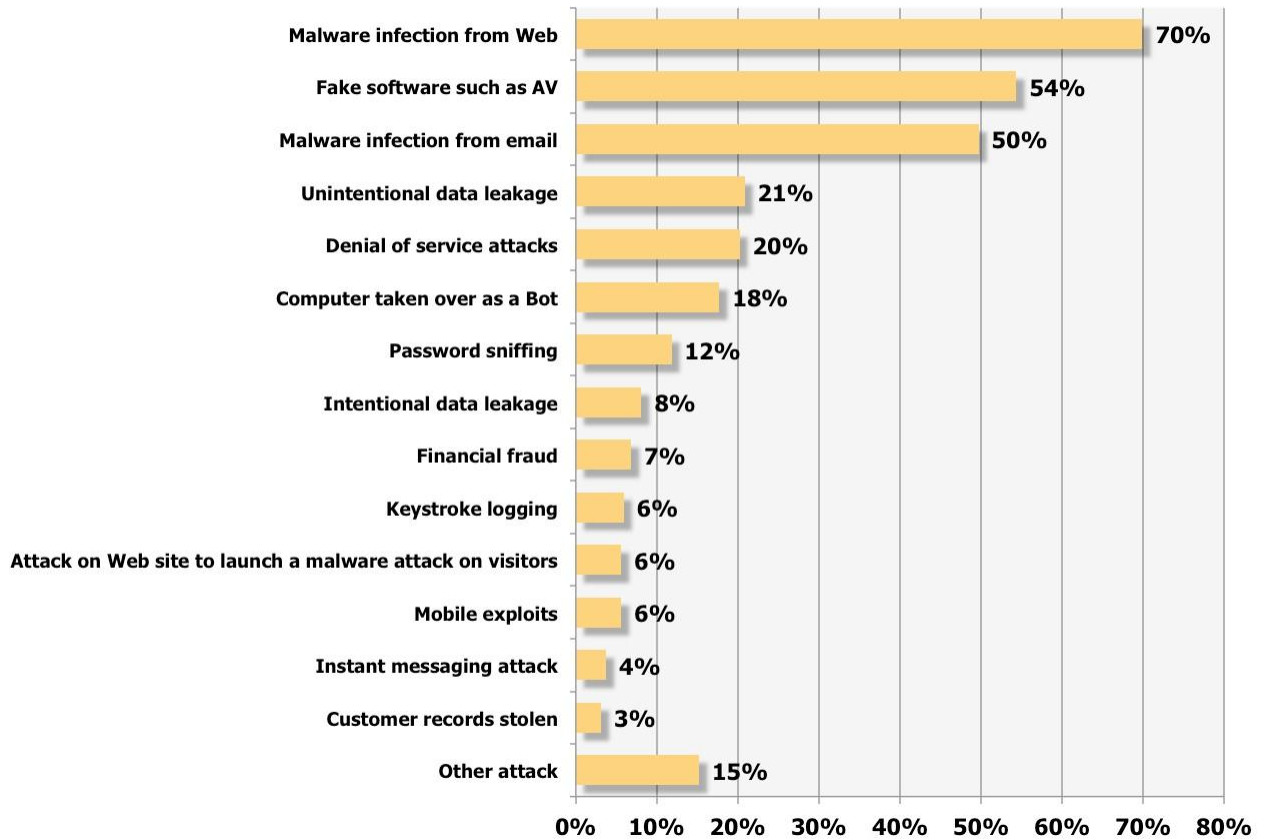
MOST HAVE EXPERIENCED MALWARE ATTACKS

Our research found that 78% of the organizations surveyed had experienced at least one malware attack during the preceding 12 months, and that each organization had experienced a median of five attacks during this period. This means that the typical organization experiences a malware attack every 73 days.

We found wide variability in the number of attacks across different industries. For example, among high-tech services providers, we found a median of “only” two malware attacks during the previous 12 months. On the other end of the spectrum were respondent organizations in educational institutions, which had a median of 12 attacks during the same period. Financial services and government organizations, as other leading industries represented in the survey, had a median of four and 10 attacks, respectively, during the previous 12 months.

Attacks come in a variety of forms, although the most common have been malware infection from the Web, introduction of fake software (i.e., scareware) or malware infection from email, as shown in the following figure.

Types of Attacks Experienced During the Past 12 Months
Percentage of Companies Reporting an Attack



Most organizations have seen no improvement or experienced an increase of malware infections over time. Our research demonstrated that in 64% of surveyed organizations, the malware problem remained about the same for the past 12 months, but for 27% it worsened (we found no appreciable difference in this figure across various industries). Only 9% of organizations reported that the problem has actually decreased.

However, these figures are quite different for organizations that believe their security solutions are sufficient. For example, only 6% of organizations that are satisfied with their current security solutions report that malware is getting worse—less than one-quarter of the overall average of respondents. Not surprisingly, then, the more robust the malware solution, the more satisfied organizations will be.

DIRECT COSTS OF MALWARE

The direct cost of malware can vary widely, from zero to hundreds of thousands or even millions of dollars. For example, the following organizations, representing a small fraction of malware victims that have had corporate funds stolen from them, lost a combined \$5.7 million as a direct result of malware infecting one or more computers on their corporate network:

- Hillary Machinery: \$800,000ⁱ
- Catholic Diocese of Des Moines, Iowa: \$600,000ⁱⁱ
- Patco: \$588,000ⁱⁱⁱ
- Western Beaver County School District: \$700,000^{iv}
- Experi-Metal, Inc. : \$560,000^v
- Village View Escrow: \$465,000^{vi}
- Unidentified construction company in California: \$447,000^{vii}
- Choice Escrow: \$440,000^{viii}
- Government of Bullitt County, Kentucky: \$415,000^{ix}
- Town of Poughkeepsie, New York: \$378,000^x
- Unidentified solid waste management company in New York: \$150,000^{xi}
- Unidentified law firm in South Carolina: \$78,421^{xii}
- Slack Auto Parts: \$75,000^{xiii}

In many cases, these organizations were targeted specifically through spear phishing attacks directed at the company's CFO, CEO or other senior-level employee who accesses the corporate banking system. Using the Zeus botnet, for example, a cybercriminal can infiltrate a single company computer and install a keystroke logger that will permit the hacker to access the corporate banking system. Once there, he or she can transfer funds to "mules," often located in the same country as the victim, who then wire the money to their handlers in Eastern Europe or other locations. In research for this report, we found that a mean of 7.9% of the incidents that targeted the respondents' organizations were specifically crafted for the individual. This lowers any suspicion on the part of the user and increases the ultimate success of the malware attack.

Our research also determined that while 30% of organizations surveyed reported no financial impact arising from an attack, 44% told us that the cost of an attack was as high as \$10,000 for a single attack. Another 15% estimate the financial impact at between \$10,000 and \$50,000. Interestingly, but not surprisingly, while 70% of organizations reported some financial loss following a malware attack, 41% of financial services reported a financial impact resulting from a malware attack as high as \$10,000 – another 27% reported incurring financial consequences as high as \$50,000 and 14% reported costs of more than \$50,000.

INDIRECT IMPACTS OF MALWARE

In addition to the loss of funds experienced by many malware victims, there are a number of other costs, many of them indirect and perhaps more difficult to quantify, but no less serious:

- **IT and other labor costs**

Our research found that there were significant costs associated with IT labor as a result of malware infiltrations. For example:

- 76% of the organizations in our survey that had been attacked had to reimage computers, 37% had to change their security policies
- 32% had to provide additional training
- 22% attempted to do their own forensics to solve the problem
- 12% consulted legal counsel

Additionally, we found that the typical malware attack requires a mean of 27.5 IT person-hours to remediate, and 12% of employees in the average victimized organization cannot work normally while the problem is being remediated. Our research showed that approximately two-thirds of the cost of a malware attack in a typical organization is related to IT labor costs.

We found some variability in terms of the IT labor required to remediate the problems associated with malware. For example, high-tech services companies spent a mean of 15.8 person-hours remediating malware attacks, while financial services companies spent more than twice as much time at 39.5 hours.

- **Direct IT costs**

Our research also found that:

- 51% of attack victims had to install additional security software after an attack
- 20% installed additional hardware

- **Lost revenue opportunities**

In addition to the actual labor, software and hardware costs of an attack, there are consequences that are difficult to quantify. These include the lost revenue that results when some customers, after learning of a company's security breach, will be reluctant to do business with that company again.

- **Bad press**

In an age of almost instant press coverage from traditional media, as well as “unofficial” coverage from sources like Twitter users, bad news travels very quickly and can have a major, if difficult to quantify, impact on purchase decisions. For example, the Dropbox security failure on June 19, 2011, although not caused by malware, generated these comments on Twitter:

- “sorry #dropbox, that's one too many giant fails. i'm leaving you for #spideroak”
- “@Dropbox dropping the ball leaving 25million customers' online folders open for all for 4 hours.”
- “#Dropbox made a huge mistake during last weekend's upgrade leaving all of its user accounts unlocked.”
- “Okay, I'm leaving Dropbox now. It's over, you and me.”
- “Dropbox leaving user accounts unlocked might be the trigger to try out SpiderOak or Wuala”
- “I'm leaving Dropbox. Join me on Spideroaks and we both get 1GB free storage for life!”

- **Other costs**

Other malware-related costs that victimized organizations will incur include internal meetings to discuss the problem, unforeseen costs such as employees leaving early while their computers are being repaired, additional help desk calls, emails and calls from worried customers and business partners, and overall loss of goodwill.

THE COST OF MALWARE REMEDIATION: A SCENARIO

To demonstrate the costs associated with malware remediation in terms of the direct, non-catastrophic costs of dealing with the aftermath of an attack, we have developed the following scenario for a 500-person company using data generated from the survey, as well as a few additional assumptions:

- The fully burdened annual salary of an IT staff person is \$80,000 and the cost of a non-IT employee is \$65,000.
- The following tasks will be required following a single, non-catastrophic attack:
 - Reimaging machines: 25 IT person-hours required; occurs after 76% of attacks
 - Installing additional hardware security: \$5,000; occurs after 20% of attacks
 - Installing additional software security: \$2,000; occurs after 51% of attacks
 - Providing new security services: \$1,000; occurs after 22% of attacks
 - Providing additional training: one hour of training required for 100 employees

Based on these assumptions, the total cost of remediating a single malware attack is \$3,996. If we assume, as discovered in the survey, that there is a median of five attacks per year, the total cost of remediating attacks will be nearly \$20,000 annually.

Again, it is important to keep in mind that these represent conservative estimates that do not take into account major financial losses or breaches of confidential data, both of which could increase the cost of remediation for a single attack by at least one order of magnitude.

ORGANIZATIONS THAT DO NOT ADDRESS MALWARE ARE AT SERIOUS RISK

The bottom line is that all-sized organizations across all industries are at serious risk if they do not directly and adequately address the malware problem. Dealing with the risks at a later time or devoting inadequate resources to the problem will eventually result in significant financial and other costs to an organization.

The Hurdles in Addressing Malware

WELL-FUNDED CRIMINALS CONTINUE TO DEVELOP THEIR ATTACKS

One of the fundamental problems in addressing malware is that a well-funded global criminal industry continues to increase the both the sophistication and volume of their content. For example, in 1991 IBM reported that it had captured more than 400 virus samples in its database. By 2007, 10,000 different malware files were being discovered on a typical day, a figure that swelled five times by 2010. The number of variants continues to grow, inundating many organizations' malware defenses.

The primary reason for the dramatic increase in malware is simply the value of criminals' targets. The average individual, for example, possesses several credit card accounts that can sell on the black market for anywhere from \$10 to \$90 each, while their passport information sells for more than \$1,000 in some cases. Organizations have bank accounts that if tapped, can generate hundreds of thousands of dollars in funds that can be wired out of the country long before the victim realizes a breach has occurred.

Moreover, malware is becoming more sophisticated and is able to defeat many of the defenses that have worked against it in the past. For example, some malware is now able to defeat two-factor authentication systems and malware authors are becoming more clever in their use of social engineering tricks designed to trick users. As but one example of the sophistication of newer forms of malware is Stuxnet. This particular malware was designed to target one type of Siemens controller used in Iran's nuclear weapons program and will expire in June 2012. While Stuxnet was not designed to attack companies or consumers, it demonstrates how malware can go after a very specific type of target and remain undetectable until after it has done its work.

THE MANY SOURCES OF MALWARE

As noted earlier, malware originates from a variety of sources, including: Web 2.0 applications such as social media tools, simple Web surfing, email, various cloud-based services, business-legitimate Web sites, non-legitimate Web sites, inadvertent actions by employees, Skype, infected USB flash drives, smartphones, tablets and more.

Plus, as more employees work from home one or more days per week, the corporate network is increasingly vulnerable to whatever security employees decide to install on their home computers, the firewalls they maintain on home Wi-Fi routers, the level of Wi-Fi security chosen (if they have security at all) and so forth. Additionally, in many cases, employees' families use the family computer for personal applications and the potential for malware to infiltrate the corporate network increases.

THOUSANDS OF THREATS

Many types of threats can impact organizations. Zeus, Conficker, Asprox, Autorun, Taterf, Ika- tako and different types of Trojan proxies are just a few of the malware variants that infect organizations. Furthermore, there are various types of "Mugged in London" messages that many users receive in email, ransomware that attempts to extort money from victims, clickjacking, scareware, and other threats.

MORE ENTRY POINTS FOR MALWARE

As noted earlier, there are a growing number of ways for malware to enter a corporate network, including:

- Email
- Smartphones and tablet computers
- Personal Webmail
- Web surfing
- Cloud-based services
- Social media tools like Twitter and Facebook (plus more than 1,000 other social media sites)
- Skype and other VoIP systems
- Other Web 2.0 applications
- USB flash drives
- Home computers
- Unprotected Wi-Fi networks and router firewalls
- Consumer instant messaging clients

The number of entry points is drastically higher today than just a few years ago. Unfortunately, many of the solutions organizations have chosen to protect their organizations have not kept pace with the level of risk introduced by the rapid growth of devices and platforms in use.

MORE LOCATIONS AND DEVICES MEAN LESS IT CONTROL

Now, employees are more geographically distributed, making protection much more difficult than in the past. Moreover, until recently, the firewall surrounded a corporate data center that contained servers, data, desktop computers and other key infrastructure elements, creating a barrier between the internal network and the outside world. While the introduction of new devices and platforms into the workplace is not without its benefits, it does make defending against malware significantly more challenging. The bottom line? The continuing geographic dispersion of employees, coupled with the increasing use of personal devices for work-related tasks, means that IT has less control over user behavior and modern platforms.

How Protected Is Your Organization?

NOT ALL SOLUTIONS ARE CREATED EQUAL

Various independent testing organizations, as well as the personal experiences of most IT administrators, reveal that there is a wide degree of efficacy in malware detection and remediation solutions. This fact has not been lost on the majority of our survey respondents. While only 22% of respondents agreed or strongly agreed with the statement that “no vendor’s security solutions are really that much better than others,” 61% disagreed or strongly disagreed. Only 17% were neutral on this issue.

THE CONSEQUENCES OF INADEQUATE MALWARE PREVENTION

In addition to the previously discussed impacts of malware attacks, there are some very serious, industry-specific ramifications. For example, a data breach can result in violation of one or more of the following regulatory requirements designed to protect consumer, financial, patient and other sensitive information:

- **Payment Card Industry Data Security Standard (PCI DSS)**
PCI DSS encompasses a set of requirements for protecting the security of consumers’ payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.
- **Gramm-Leach-Bliley Act (GLBA)**
GLBA requires that financial institutions protect information collected about individuals, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule (16 CFR Part 313) and the Safeguards Rule (16 C.F.R. Part 314). GLBA also addresses steps that companies should take in the event of a security breach, such as notifying consumers, notifying law enforcement if the breach has resulted in identity theft or related harm, and notifying credit bureaus and other businesses that may be affected by the breach.

- **Health Insurance Portability and Accountability Act (HIPAA)**
HIPAA addresses the use and disclosure of an individual's health information. It defines and limits the circumstances in which an individual's protected health information (PHI) may be used or disclosed by covered entities, and states that covered entities must establish and implement policies and procedures to protect PHI. Penalties for violations are up to \$25,000 and \$1.5 million, depending on when the violations occurred.
- **Personal Information Protection and Electronic Documents Act (PIPEDA)**
PIPEDA is a Canadian privacy law that applies to all private companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely. Canada's Privacy Act, in place since 1983, protects the personal information collected by government institutions.

Across our entire base of survey respondents, we found that:

- 17% reported suffering some sort of regulatory or compliance violation as a result of a malware attack.
- High-tech services organizations reported the lowest incidence of such violations at 11%.
- Government organizations reported the highest incidence at 28%

A malware-induced data breach can result in non-compliance with a multitude of other federal, state, and provincial statutes. The consequences of non-compliance with data breach notification laws, now in effect in 46 US states and one Canadian province, means that breached organizations must at least notify victims (and possibly take other remedial actions), which can potentially cost millions of dollars per incident.

A STRATEGY FOR COMBATTING MALWARE

Osterman Research recommends that organizations seriously consider addressing malware prevention, detection, and remediation in two ways:

- **Train end users**
Users should be trained on how to properly surf the Web, what they should do when they encounter a blended threat (a spam email that contains a link to a Web site), how they should be wary of emails whose source is not known, how to spot phishing attempts, and the like. Proper training can prevent some malware attacks and can thwart some social engineering techniques used by malware authors.
- **Address the long-term, strategic impacts**
However, because no amount of user training can address all of the malware issues that organizations face, the right technologies must be deployed that can detect malware and prevent it from harming an organization. This includes addressing malware detection and remediation at every ingress point, including email, smartphones, Web browsers and the growing multitude of other platforms from which malware can enter the network.

The Benefits of Addressing Threats Proactively

With the right user training, corporate policies, and technology, organizations can effectively address the malware problem. Benefits of serious, proactive malware prevention include:

- **Protection from catastrophic financial** events such as the loss of hundreds of thousands or millions of dollars drained from corporate accounts.
- **IT labor cost savings** from minimized need to remediate malware-related problems.
- **Improved employee productivity** that comes from reduced malware-related outages and resulting downtime.
- **Preservation of corporate reputation** and elimination of the need for damage control activities often required after a malware attack.

To achieve these benefits, decision makers must address the malware problem with sufficient attention and resources. Those who do not are likely to incur serious consequences.

About M86 Security

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: www.m86security.com.

© 2011 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

ⁱ <http://rixstep.com/1/1/20100126,00.shtml>

ⁱⁱ <http://krebsonsecurity.com/tag/catholic-diocese-of-des-moines/>

ⁱⁱⁱ <http://www.networkworld.com/news/2009/092409-construction-firm-sues-after-588000.html>

^{iv} <http://www.post-gazette.com/pg/09195/983738-57.stm>

^v http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000_

^{vi} <http://krebsonsecurity.com/2010/06/e-banking-bandits-stole-465000-from-calif-escrow-firm/>

^{vii} <http://www.technologyreview.com/computing/23488/?a=f>

^{viii} http://www.bankinfosecurity.com/articles.php?art_id=3159&opg=1

^{ix} http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html

^x http://www.computerworld.com/s/article/9153598/Poughkeepsie_N.Y._slams_bank_for_378_000_online_theft

^{xi} <http://www.suite101.com/content/protect-yourself-against-banking-crimeware-a156086>

^{xii} http://www.abajournal.com/news/article/doj_says_massive_decade-old_botnet_helped_web_thieves_steal_millions/

^{xiii} http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html