

LOWERING IT COSTS: HOW TO REDUCE THE NEED FOR DESKTOP REMEDIATION AND SHAVE MILLIONS OFF IT EXPENSES

THE CORRELATION BETWEEN DESKTOP REMEDIATION AND MALWARE

Every year, organizations spend significant time, resources and money to remediate damaged desktop systems and the problem is only increasing as the malware problem grows. The costs associated with re-imaging and remediating desktops often exceed established IT budgets, which in turn, reduces funds or resources available for strategic or core IT projects. Ultimately, this can impact an organization's bottom line. The specific causes of these problems are not always obvious; however, more often than not, malware, especially next-generation threats, is the culprit, damaging systems, stealing valuable information and leaving PCs inoperable without IT support intervention.

Though the exact costs of PC remediation vary by organization, one thing is clear: an average malware attack today can cause significant damage, which forces organizations to expend higher percentages of their resources and budgets than anticipated. This white paper will help organizations understand and quantify how next-generation threats influence remediation costs and find a solution to minimize those costs and maximize efficiency.

How Pervasive Is The Problem?

The malware problem is not a new challenge. But the severity is escalating, not only for executives and other business managers who worry about corporate reputation, compliance, data loss and other corporate-level concerns, but for technical support and IT teams, who are forced to stretch their resources and budgets to repair, and sometimes replace, the increasing number of damaged, malware-infected systems.

Underscoring this, industry research by M86 Security and other sources consistently report high numbers of infected PCs in organizations. For example, Gartner estimates that 4–8% of an organization's PCs are infected with a bot at any given time.¹ Microsoft reported that 5% of computers—one out of every 20—are infected; and with not just one but an average of 3.5 malware applications each.² Moreover, a research survey conducted by Osterman Research and M86 Security shows that 70% of organizations surveyed had been affected by Web-based malware in the past 12 months.³

How much do these malware infections cost to remediate? One security vendor reports the average cost of resolving/remediating individual malware incidents is \$334 per case,⁴ while a joint Osterman-Edgewave-McAfee report puts a conservative estimate of \$150-\$200 on each desktop incident.⁵

In reality these attacks probably cost organizations substantially more over the long term than is reported because they amass measurable hard costs as well as less quantifiable soft costs and lost opportunities. For example, NetworkWorld published that almost 40% of enterprise IT trouble tickets are from spyware alone,⁶ which means these engineers are being paid to deal with malware-inflicted damage while more strategic projects go unaddressed.

Malware Infection Symptoms Can Underlie Bigger Problems

Britta Smith, a University of Washington junior, was capable of operating a PC; however, her computer had been seriously infected by malware. She became aware of the infections through the constant spyware, pop-ups, pop-unders and adware. It had

become so pervasive that she didn't know how to fix the problem. In Idaho, an office manager claimed that spyware had become her company's number one maintenance problem. Additionally, a University District shop owner was inundated with pop-ups every time he started his office PC.⁷

These are common issues for office workers and other users, and in these examples, the infections had side-effects that were obvious. What these users may not realize is that the malware could be much more severe than these symptoms suggest, and without remediation, the attacks could cause serious damage with long-term consequences.

THE DEBILITATING EFFECTS INFECTED SYSTEMS HAVE ON BUSINESSES

Most people are familiar with the more-publicized consequences of malware-infected systems. These include compromised confidential customer information, mishandling of Personally Identifiable Information (PII), stolen funds and theft of intellectual property. However, ineffective security also leads to additional costs that are often overlooked, such as crippled productivity, lost revenue and escalating IT operations budgets, all of which can be staggering. An infected machine requires an IT staff investment for remediation, as well as the user's time to reinstall programs and restore the computer to its former state. A survey of 820 IT decision makers in SMB organizations in the United States, the United Kingdom and Australia indicates that re-imaging infected machines alone, averages more than 17 hours per month. And in companies where at least 25% of employees access the server remotely, repair time takes even longer.⁸

Soft costs often encompass personal as well as company brand, image and reputational damage, and loss of trusted relationships with customers and partners. It's difficult to be comfortable doing business with a company or an agency that can't protect proprietary or confidential information. Opportunity costs also take a toll. The IT person remediating the system could have otherwise spent that time proactively improving enterprise security defenses rather than reactively responding to a malware infection. All the while the user, whose machine was infected, could have been performing normal job functions, uninterrupted.

UNDERSTANDING THE ROOT CAUSE: HOW NEXT-GENERATION ATTACKS ARE SUCCESSFUL

M86 Security estimates that 92% of all malware comes from the Web. Since 2007, the cybercrime industry has grown more than 400%, with tens of thousands of malware variants discovered every day.

Gartner acknowledges a change in the threat environment that has attributed to this huge increase in malware incidents. M86 refers to this change as next-generation threats: sophisticated, targeted, and socially well-engineered attacks designed to avoid traditional security measures and steal sensitive data for financial or competitive gain. Examples include:

- Phishing and Blended Threat Emails
- Advanced Persistent Threats
- Targeted Attacks
- Zero-day Attacks
- Advanced, Polymorphic Malware

Next-generation attacks are specifically designed to bypass almost every existing Web security solution to infect a system; remain there undetected for a period of time; and then to collect something valuable to the criminal such as sensitive information or access to finances. Cybercriminals continuously refine these attacks to achieve even higher success rates, greater profitability and lower detection rates.

Understanding the Malware Gap

Most Web security vendors offer solutions that detect less than 50% of next-generation threats before they enter an organization's network, leaving a "malware gap" on networks and PCs.

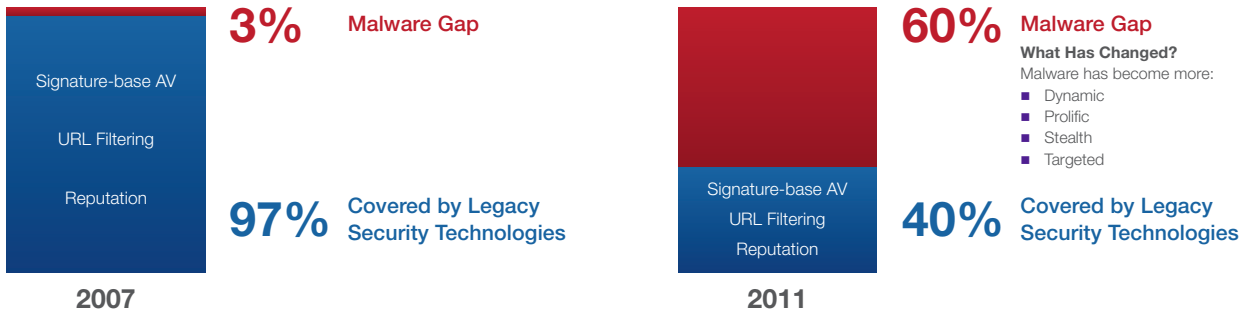
Underscoring this, a Cyveillance Cyber Intelligence Report found that traditional anti-virus products cannot adequately protect against new and quickly-changing malware threats on the Internet. An analysis measured the average daily detection rate of 14 of the most widely-used anti-virus products against real-time confirmed attacks for six months. They found that less than half of the malware threats were detected. Additional testing found that the leading six anti-virus products demonstrate approximately a 50% chance of protection—even a week after the release of new malware threats.⁹

Further supporting this, M86 Security found similar results in its own testing, noting that as much as 60% of malware, specifically targeted next-generation threats with new malicious code, evades most other Web security solutions.

This is because technologies commonly used to detect malicious attacks, such as anti-virus, Web filtering, firewalls, IDS/IPS and even most secure Web gateways, rely on matching what is scanned on a Web page to a list of identified (previously encountered) threats to a pattern of misbehavior to recognize malware and then protect against it. This is a problem because almost every type of next-generation threat uses unknown, zero-day malware that will not be on a signature list or match a pattern.

MALWARE GAP

Left by Legacy Malware Technologies



DESKTOP CLEANUP SCENARIOS: MORE THAN A NUISANCE

While re-imaging and cleaning infected desktops is typically viewed as a hassle for IT teams and a productivity killer for users, these tasks add up to significant financial costs. And that is exactly what happened in the following scenarios.

A 100,000-employee financial institution needed to constantly reimage desktop PCs, actions that were attributed to malware infections. The IT team estimated a steady workload of approximately 40 PCs daily, or 12,000 infected PCs per year, a crippling demand considering this was time spent on desktop reimagining alone. Once the team calculated the time and money spent re-imaging PCs, they realized they were looking at a \$3.02M annual figure. By comparison, Gartner's estimate that 4-8% of enterprises PCs are infected would have put this number at 8,000, which is considerably less than the actual 12,000 number confirmed.

	Customer One	Customer Two
Estimate Infected PCs per Day	40	133
PC Re-imaging & Help Desk Costs per Year	\$3.02M	\$10.0M
Gartner Estimate 8% Infected PCs	8,000	24,000

Another 300,000-employee company, also in the finance industry, experienced help desk costs of \$10M per year for support calls on malware-infected PCs. This organization outsourced its technical support services to a third party who charged per call. At \$10M per year and climbing, the IT budget was being monopolized by these

routine support tasks. This was a huge problem, especially for a financial organization that relies on this budget for strategic and competitive purposes such as implementing innovative technologies for online and mobile banking. This 300,000-user organization estimated 133 infected PCs per day or 39,900 per year, as compared to Gartner's 4-8% estimate, which would have put this number at 12,000-24,000 potentially, infected PCs.

Neither of these financial institutions was operating unprotected. Both companies had some of the security industry's largest vendors' solutions fully deployed and running on the network and desktop levels, yet they still ended up with millions of dollars in malware-cleanup costs. These are real-world examples of the malware gap mentioned previously in this paper. Because detection rates have fallen to less than 50% with most security solutions, enterprises are falling victim to malware, and this equates directly to millions of dollars in remediation costs per year.

WHY "GOOD ENOUGH" IS NO LONGER GOOD ENOUGH

Web security solutions are inadequate to protect from today's next-generation threats. It is important to understand both the strengths and weaknesses of the primary security techniques used by most vendors.

Eric Olson, Cyveillance Vice President of Solutions Assurance, says that anti-virus and firewall systems, while necessary, are insufficient defenses because they are reactive. Malware writers own anti-virus software too and know how to counter it, explained Olson. They can test existing anti-virus and firewall technologies, run malware samples against them, and then make necessary adjustments to ensure a successful attack.⁹

Another approach used by some vendors is more effective at identifying advanced malware; however, it identifies these threats by catching them once they attempt to "phone home" from an

organization's network back to the criminal's Command and Control Server. The downside to this method is that the malware is essentially allowed to infect a network or system in order to be identified. Although the detection rates are high, by the nature of the approach, an organization's desktop remediation costs will be exorbitant, especially compared to an effective, inline solution that stops malware before it infects a network.

It is crucial for IT teams and organizations to understand the consequences of relying on security solutions that fail to fully protect their systems. If the most popular technologies on the market only detect half of today's malware before it enters an organization's network, then organizations are highly vulnerable to the costs and damage inflicted by these attacks.

WHAT WORKS: PREVENTING MALWARE AND REDUCING DESKTOP REMEDIATION

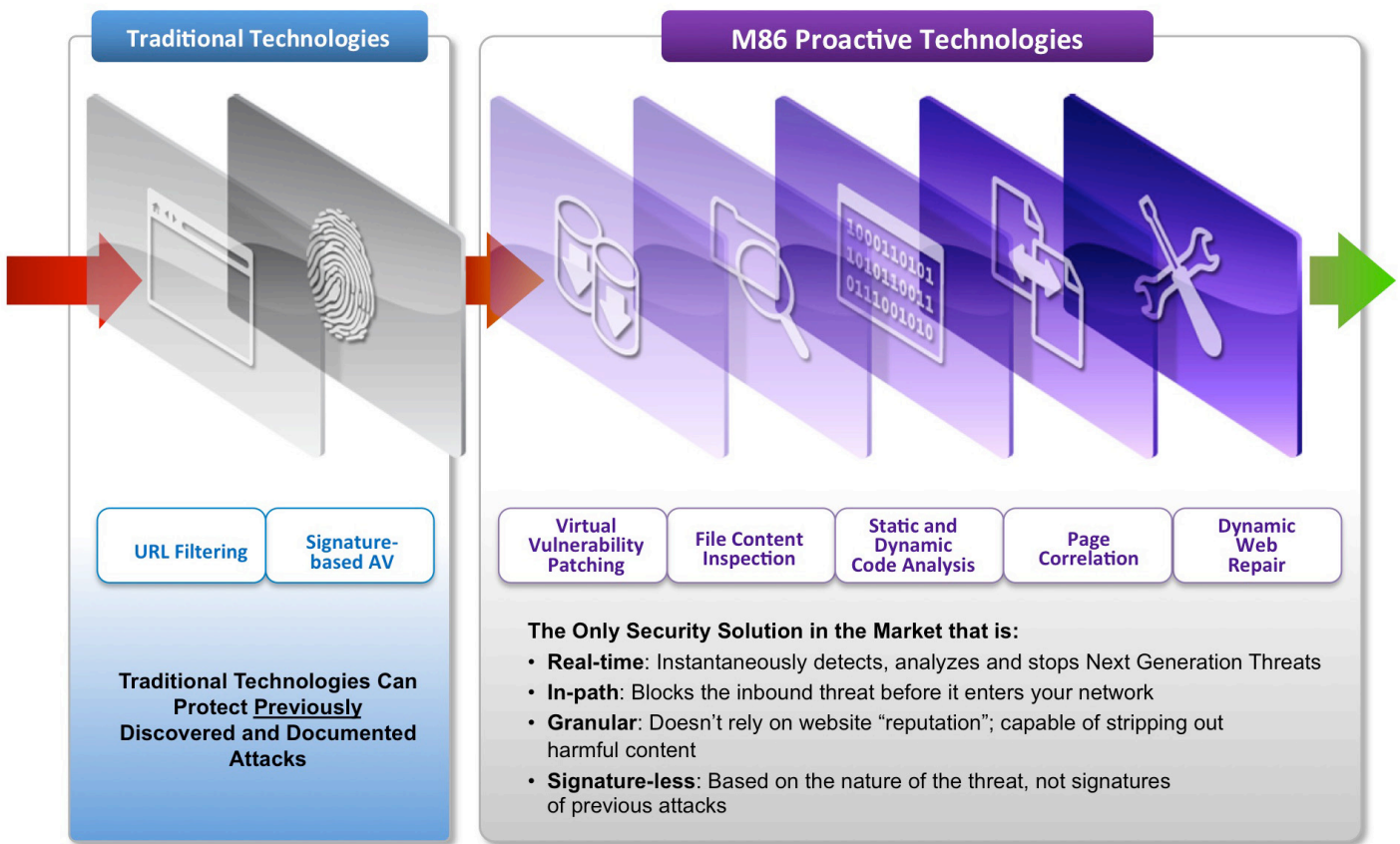
Stated earlier, the Internet is the primary attack vector for malware, with approximately 92% of all malware attacks occurring through the Web. By instantly analyzing Web code as it is visited by users,

and by determining the intent of any remaining content that is not already identified as known malware or vulnerabilities, the M86 Secure Web Gateway (SWG) detects all forms of malware, including next-generation threats.

How the M86 SWG Detects Malware

The difference between M86 Security solutions and other vendors, even the largest vendors in the industry, is that the M86 SWG is the only solution that can determine the intent of the code on a Web page. What is the code trying to do on a potential victim's computer? Are these the actions of safe, legitimate software or is the code trying to perform a suspicious action, copy files, open settings or exploit a known vulnerability? By focusing on the intent or behavior of the code, M86 Security's real-time, layered technologies are effective against even the most sophisticated targeted attacks. It is the most accurate, intelligent Web security solution on the market and provides the only protection from today's next-generation threats.

The diagram below shows how Web traffic moves through the layers in the M86 SWG's anti-malware engine to detect malware or malicious activity.



The Proof

The 100,000-user financial institution that spent an estimated \$3.02M annually to remediate malware-infected systems (discussed previously) ran a side-by-side-by-side comparison of three Web security vendors' solutions: a Web security appliance and a proxy AV, along with the M86 SWG. For this test, the organization used 2,500 URLs that had been recently-identified as containing malicious content. After the 2,500 URLs were run through each solution, the first vendor's Web security appliance identified two incidents of malware, the second vendor's proxy AV found five occurrences and the M86 SWG recognized 106 malicious URLs. These results were analyzed for over-blocking or under-blocking. The outcome of the analysis was interesting: It turns out that both catches from the first vendor and four of five catches from the second vendor were all false positives, while all 106 of M86 Security's flagged URLs were accurately identified as malicious sites.

Although this outcome is to be expected when a reactive, list-based technology such as that used by the two competitive vendors is compared to a real-time, intelligent security, like that used by M86 Security, the vendors of the lower-performing solutions asked for a second side-by-side-by-side comparison. This time, 10,000 URLs were selected from the 100,000-user organization's production environment. This represented a snapshot of general browsing activity within the organization. These were not necessarily URLs that recently had been identified to carry malware. The results of the second test came back with no blocks by either of the two competitive solutions but with two blocks by M86 Security. Another analysis revealed that the M86 blocks were accurate, while the other vendors had both missed these malicious URLs. Initially, this may sound insignificant; however 10,000 URLs can represent one second of Internet traffic at some points during the day for this organization. Multiply two malware cases in one second by a full day's worth of Internet traffic and you can quickly see how serious and expensive the problem can be. In this case, the company could save more than \$3M per year, with a quick ROI of less than one year by using the M86 SWG.

RECOMMENDATIONS

Evaluate Potential Solutions Thoroughly

Many organizations' IT decision makers, driven by time and budget constraints, now select Web security solutions hurriedly, without first testing and researching several solutions for the validity of their claims. Almost every vendor claims to have the "be all, end all" Web security solution, but as discussed previously, most cannot truly prevent today's evasive targeted malware. Instead of relying on paper-based exercises to select one product for which to perform proof-of-concept, it is crucial for organizations to fully evaluate several products in efforts to not just believe they are choosing the best protection, but to know it. By selecting the most accurate, most effective solution, organizations will save significant time and money in both the near and long term.

Look for Technologies that Provide High-level Protection

Most standard Web security solutions provide low- to mid-level malware defense by using technologies that rely on signatures, IP reputation or other reactive methods. To fully protect from malware, and consequently, lower the costs of remediating malware-infected desktops, organizations need proactive, signature-less security that analyzes code and detects malware in real time. This kind of intelligent security prevents even next-generation malware from infiltrating systems and networks because it operates "in path," actively scanning and blocking code as it executes before malware can infect a network.

CONCLUSION

Web-based attacks, especially those using next-generation threats have exploded in frequency, and more importantly, are extremely successful. Not all Web security solutions are equal, though many purport to provide superior protection. By taking time up front to fully investigate and test potential solutions before purchasing and implementing them, organizations can be empowered to make informed, cost-effective decisions about their IT security investments. By selecting an intelligent solution that is truly effective, organizations can prevent malware infections proactively, and therefore significantly reduce the quantity and frequency of costly remediation, including reimaging, of desktops. In addition, users will be able to maintain productivity, and IT teams can spend their valuable time on strategic duties, increasing efficiencies and providing a significant, long-term cost savings.

REFERENCES

1. Secure Web Gateways: Intelligently Defending Against the Web 2.0 Threat, Gartner Presentation, 2011
2. Microsoft Mulls Malware, July 21, 2011
3. The Global Malware Problem: Complacency Can Be Costly, Osterman Research and M86 Security, 2011
4. Norton Cybercrime Report, 2011
5. Quantifying the Costs and Benefits of Web Security, Edgewise/Osterman Research webinar, June 30, 2011
6. Why Network Execs Need to Care About the Applications on the Network, Network World
7. The Seattle Times, Geek Squad Has Hands Full with Malware, October, 11, 2004
8. Webroot Report, February 2011
9. Cyber Intelligence Report: A Cyveillance Report, October 2010

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations.

Simply contact us or visit:

www.m86security.com/downloads.

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.



Corporate Headquarters

8845 Irvine Center Drive
Irvine, CA 92618
United States

Phone: +1 (949) 932-1000
Fax: +1 (949) 932-1086

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific

Suite 3, Level 7 100 Walker St.
North Sydney NSW 2060
Australia

Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899