



Trend Micro™ Smart Protection Network Security Made Smarter.

Content Security 

 Core Technology

A Trend Micro White Paper | June 2008

I. EXECUTIVE SUMMARY	3
II. INTRODUCTION: THE DIGITAL UNDERGROUND ECONOMY	3
III. THE CHANGING THREAT LANDSCAPE—SECURITY CHALLENGES.....	5
Combined Threats	5
Explosion of Web Threats.....	5
IV. The Conventional Approach—Pattern-Based Solutions	7
Deployment Issues	7
IV. A NEW APPROACH—TREND MICRO SMART PROTECTION NETWORK.....	7
Web Reputation Technology	8
Web Reputation Technology	9
Email Reputation Technology.....	9
File Reputation Technology	9
Correlation Technology with Behavior Analysis.....	10
Feedback Loops	11
Threat Intelligence	11
V. CASE STUDY—THE BRAZILIAN TAX SCAM	12
The Problem	12
The Solution	13
VI. CONCLUSION.....	14
VII. ABOUT TREND MICRO	14



I. EXECUTIVE SUMMARY

As the underground economy has grown and prospered, cyber criminals have developed increasingly sophisticated malware as tools of their trade. Yet, as these criminals prosper, businesses and consumers alike are suffering financial losses, identity theft, and damaged reputations, creating a security environment that is ripe for change. Security professionals are scrambling to catch up—both with the newest malware variations and with the exploding number of Web threats. As threats have increased in number and complexity, conventional, pattern-based anti-virus protection is falling short and security update deployment issues are impacting network and system performance.

Clearly, a new approach is needed to combat evolving Web threats. Trend Micro offers that approach to threat protection today—with the Trend Micro Smart Protection Network, a next-generation cloud-client content security infrastructure designed to protect customers from Web threats. The Trend Micro Smart Protection Network combines Internet-based (“in-the-cloud”) technologies with lighter-weight, clients to help businesses close the infection window and respond in real time before threats can reach a user’s PC or compromise an entire network.

Trend Micro leverages patent-pending technology to correlate the threat data gathered through a network of proactive email, Web, and file reputation technologies, Web Crawlers, honeypots and global threat sensors of customers, partners, and threat research and support centers to combat even the most sophisticated sequential and blended threats. Built-in feedback loops and communication between Trend Micro products and services ensure automatic and immediate protection against the latest threats and provide “better together” security—much like the neighborhood watch crime-fighting systems that exist today in many communities.

This white paper provides an overview of today’s dangerous cyber crime world and outlines the challenges that security professionals face in developing solutions to address the growing number and variety of Web threats. Finally, this paper explores how the Trend Micro Smart Protection Network can deliver next-generation security to automatically protect digital information wherever users connect.

II. INTRODUCTION: THE DIGITAL UNDERGROUND ECONOMY

In recent years, the Internet security landscape has changed dramatically. The days of “hobbyist” virus writers causing outbreaks as a nuisance or show of bravado have passed. Profit-driven cyber criminals lurk behind most Web threats today, creating a new generation of malware that drives a powerful underground economy. Consumer Reports projects that U.S. consumers lost more than \$7 billion over the last two years to viruses, spyware, and phishing schemes.¹ In addition, for the 16-month period ending in mid-2006, the nonprofit Privacy Rights Clearinghouse reported that criminals compromised the identities of more than 85 million Americans, stealing social security numbers, contact information, and credit card numbers. Financial repercussions of identity theft are considerable—in the United States, \$31,000 is cited as the average amount lost in each case, counting losses to companies, as well as individuals.²

Businesses also suffer financially. In 2006, U.S. retailer, TJ Maxx, experienced a large-scale security breach when cyber criminals stole more than 45 million customer credit and debit card numbers causing financial losses totaling close to \$256 million—not to mention damage to the company’s reputation and the negative impact on consumer confidence.³ Malware clean-up presents additional, costly challenges. In some cases, Web threats may result in a system infection that is so extensive (i.e. via a rootkit in which the system file is replaced) that conventional uninstall or system cleaning approaches become useless. Infected systems often require a complete system recovery, in which the operating system, applications, and user data must be reinstalled.



TREND MICRO™ SMART PROTECTION NETWORK— SECURITY MADE SMARTER.

Data leaks are an additional business concern when employees unintentionally expose confidential information to unauthorized parties, or external hackers or thieves break into corporate networks or physically enter corporate premises to steal data. Criminals steal laptops and USB devices or purchase stolen property containing personal data for exploitation or financial gain. In addition, cyber criminals remotely siphon data using malicious software to perform their dirty work by infecting a system and then transmitting sensitive data back outside a company's security boundaries. According to the Ponemon Institute, the average cost to a business for each compromised customer record is \$197, with the total cost of a data breach averaging \$6.3 million.⁴ Additionally, each year companies incur billions of dollars in intellectual property losses to software, hardware design, drug formulations, and other trade secrets.

The underground economy flourishes, and cyber criminals profit handsomely. Ivan Maksakov, Alexander Petrov, and Denis Stepanov extorted \$4 million by unleashing a distributed denial-of-service attack on U.K. sports bookmakers.⁵ On the black market, malware such as Trojan horses used to steal online account information can fetch \$1,000-\$5,000.⁶ In addition to financial profits, some criminals spread malware for the sole purpose of increasing their Internet footprint—much like an offline brick and mortar retailer adds storefronts. Botnet herders use spam to spread malicious code that hijacks unknowing users' computers and assimilates PCs into botnets—huge collections of zombie computers that enable large-scale click-fraud and distribution of pornography, spam, and other malicious content. Today's botnets can control hundreds of thousands of infected PCs, placing computing power and network bandwidth into the hands of criminals like Jeanson James Ancheta, who earned \$60,000 by managing a 400,000-PC botnet.⁷

In addition to desktop threats, mobile devices are additional targets for hacking and denial-of-service attacks. Malware exploits mobile device operating system vulnerabilities to launch attacks. For example, a malware called Skulls deactivates all links to applications on a mobile device. Once the device is infected, users cannot send email or instant messages, and calendar functions stop working. Lost or stolen devices also pose problems for consumers and for businesses such as leaked confidential information, compliance worries, and damaged business reputations.

With the popularity of Web 2.0 and evolving exploitable application weaknesses, the boundary-less network, and a mobile workforce, the Web continues to increase significantly as a threat vector. Web threats directly impact businesses causing downtime, lost data, infections, reduced employee productivity, and time-consuming incident cleanup. Consumers suffer too—from stolen personal information and the costly consequences of identify theft, as well as from system slowdowns associated with compromised machines. As the digital underground economy grows more profitable, cyber criminals will continue to develop malware for profit, creating a critical need for adaptable security techniques and technologies that deliver better protection for all users.



III. THE CHANGING THREAT LANDSCAPE—SECURITY CHALLENGES

Combined Threats

Today's Web threats frequently combine a number of seemingly innocent programs to create an infection chain. For example, individual downloader programs, commonly used as part of Web threats, may appear benign. Yet when used to download malware onto an unsuspecting user's PC, the program becomes malicious, rendering file-based heuristic scanning ineffective. Web threats often expand this technique to include multilayered, multiprotocol coordinated attacks to avoid detection by conventional means. For instance, a cyber criminal embeds a URL in an email or instant message. The user clicks on the link to a legitimate URL that was hijacked by the cyber criminal for a few days or hours. Then an ActiveX control tests the vulnerability of the user's browser. If a vulnerability is detected, the malware attacks. If not, it downloads a file, tests for another vulnerability, downloads other files, and so on. Each session appears to be benign, but the combined activities become a coordinated attack. A single security solution is no longer enough to cover all aspects of Web threats. As a result, information security today is at a critical turning point—a new approach is needed to address today's highly sophisticated sequential and blended threats.

Explosion of Web Threats

Historically, cyber criminals have continued to advance their malware development skills, and the security industry has responded with new technologies to combat threats. Most recently, however, the explosion of new threats and the tendency toward combined threats is complicating protection efforts. For example, according to AV-Test GmbH, security vendors collected 1,738 unique threat samples in all of 1988. At that time, security professionals monitored approximately 30 signatures because samples were easily grouped into patterns.

Ten years later, the number of unique malware samples had risen to 177,615, and during the first two months of 2008 alone, 1.1 million unique samples were reported.⁸

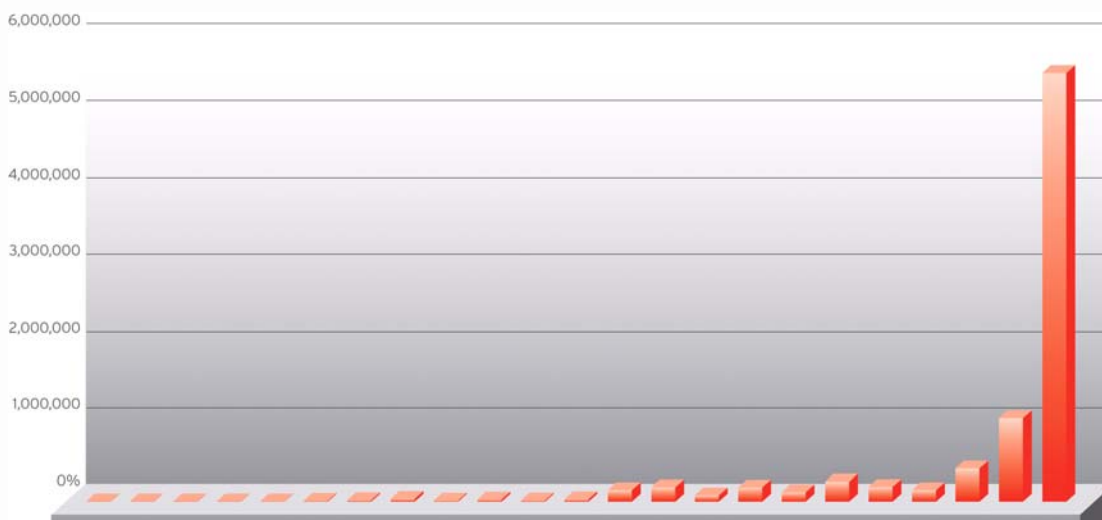


Figure 1: AV-Test.org reports 1.1 million unique malware samples during the first two months of 2008 alone.

TREND MICRO™ SMART PROTECTION NETWORK— SECURITY MADE SMARTER.

Findings from TrendLabs, Trend Micro's global network of research, service and support centers, confirm these observations. TrendLabs reported a 1,731 percent increase in Web threats between 2005 and the first quarter of 2008. TrendLabs researchers also predict that if the threat volume continues to increase at the current rate, 233 million unique threats will emerge by 2015. To be adequately protected, endpoint systems will need to detect over 26,598 new threats per hour. These numbers clearly demonstrate that the conventional approach of tracking daily threat occurrences and issuing timely security updates is becoming impossible.

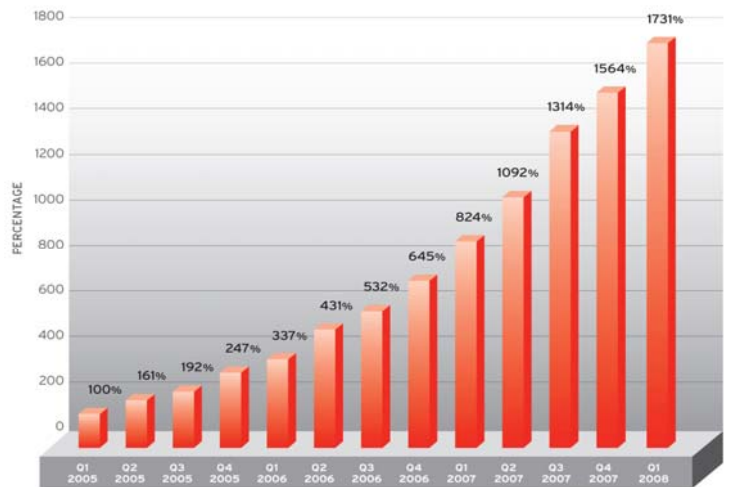


Figure 2: TrendLabs reported a 1,731 percent increase in Web threats between 2005 and the first quarter of 2008.

The threat volume is also increasing because of variants—i.e. the same Trojan can change hourly or daily in an attempt to fool security scanners. This means that millions of unique malware can, in fact, be variants of the same piece of malware. Cyber criminals are fully aware of the difficulty in issuing updates, and they use this fact to their advantage, creating new malware en masse and as quickly as possible.

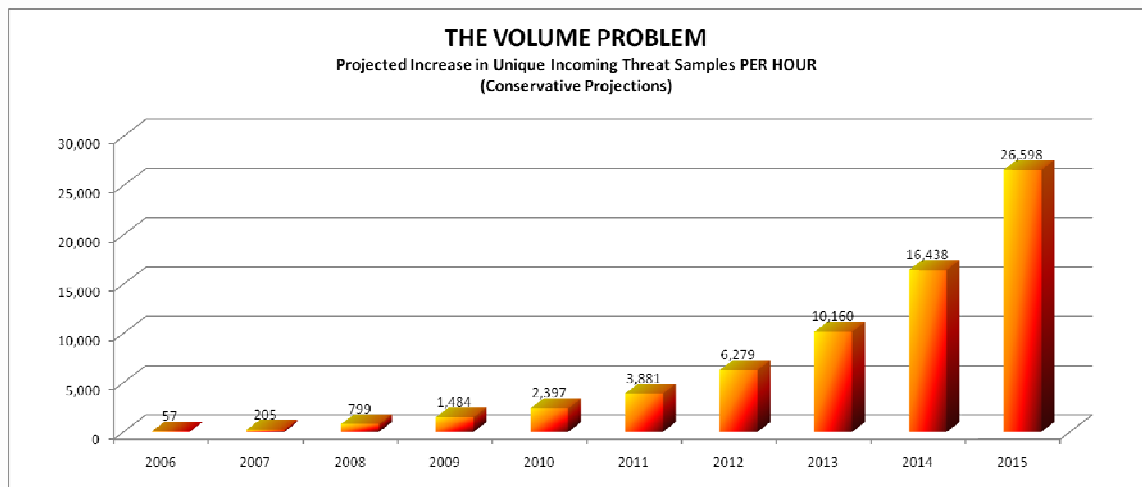


Figure 3: The volume problem



IV. THE CONVENTIONAL APPROACH—PATTERN-BASED SOLUTIONS

Conventional malware protection involves gathering samples of malware, developing patterns, and then quickly distributing these patterns to users. Because many Web threats are targeted, combined attacks, collecting samples is almost impossible. Also, the huge and growing number of variants uses multiple delivery vehicles (i.e. spam, instant messaging, and Web sites), rendering standard sample collection, pattern creation, and deployment insufficient.

Traditional virus detection processes are also challenged by a fundamental difference between viruses and evolving Web threats. Viruses were originally designed to spread as quickly as possible and were therefore easy to spot. With the advent of Web threats, malware has evolved from an outbreak model to stealthy “sleeper” infections that are more difficult to detect using conventional protection techniques.

Deployment Issues

The security industry reacted to the increasing number of malware by issuing more frequent updates. Some vendors switched from weekly updates to daily or even half-hourly updates. The consequent volume of updates has significant impact on the system and network resources required to manage pattern downloads, often leading to critical performance and cost issues. For example, imagine the bandwidth required to issue frequent updates to users' machines in a company with 250,000 global employees. A single pattern file update requires at least five hours to deploy throughout the company, and some companies receive updates as often as eight times per day to ensure they have the latest Web threat protection. Additionally, many large organizations first test pattern files in a lab or controlled environment before deploying them across their entire network. As updates grow more numerous, network administrators spend greater amounts of time managing updates. Remote or mobile workers are particularly vulnerable as they may not receive pattern file updates for hours or days, depending upon how long they are off the company network. Clearly, continual pattern file updates of this magnitude are not sustainable over time.

IV. A NEW APPROACH—TREND MICRO SMART PROTECTION NETWORK

Because conventional security solutions no longer adequately protect against the evolving set of Web threats, users need a new approach. Trend Micro delivers that approach with the Trend Micro Smart Protection Network.

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure that delivers security that is smarter than conventional approaches by blocking the latest threats before they reach a user's PC or a company's network. Leveraged across Trend Micro's solutions and services, the Trend Micro Smart Protection Network combines unique Internet-based—or “in-the-cloud”—technologies with lighter-weight clients. By checking URLs, emails, and files against continuously updated and correlated threat databases in the cloud, customers always have immediate access to the latest protection wherever they connect—from home, within the company network, or on the go.

The Trend Micro Smart Protection Network is composed of a global network of threat intelligence technologies and sensors that provide comprehensive protection against all types of threats—from malicious files, spam, phishing, and Web threats, to denial of service attacks, Web vulnerabilities, and even data loss. By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro Smart Protection Network reduces reliance on conventional pattern file downloads and eliminates the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings.



TREND MICRO™ SMART PROTECTION NETWORK— SECURITY MADE SMARTER.

The Trend Micro Smart Protection Network is composed of the following components:

- Web reputation technology
- Email reputation technology
- File reputation technology
- Correlation technology with behavior analysis
- Feedback loops
- Threat intelligence (threat collection, threat analysis)

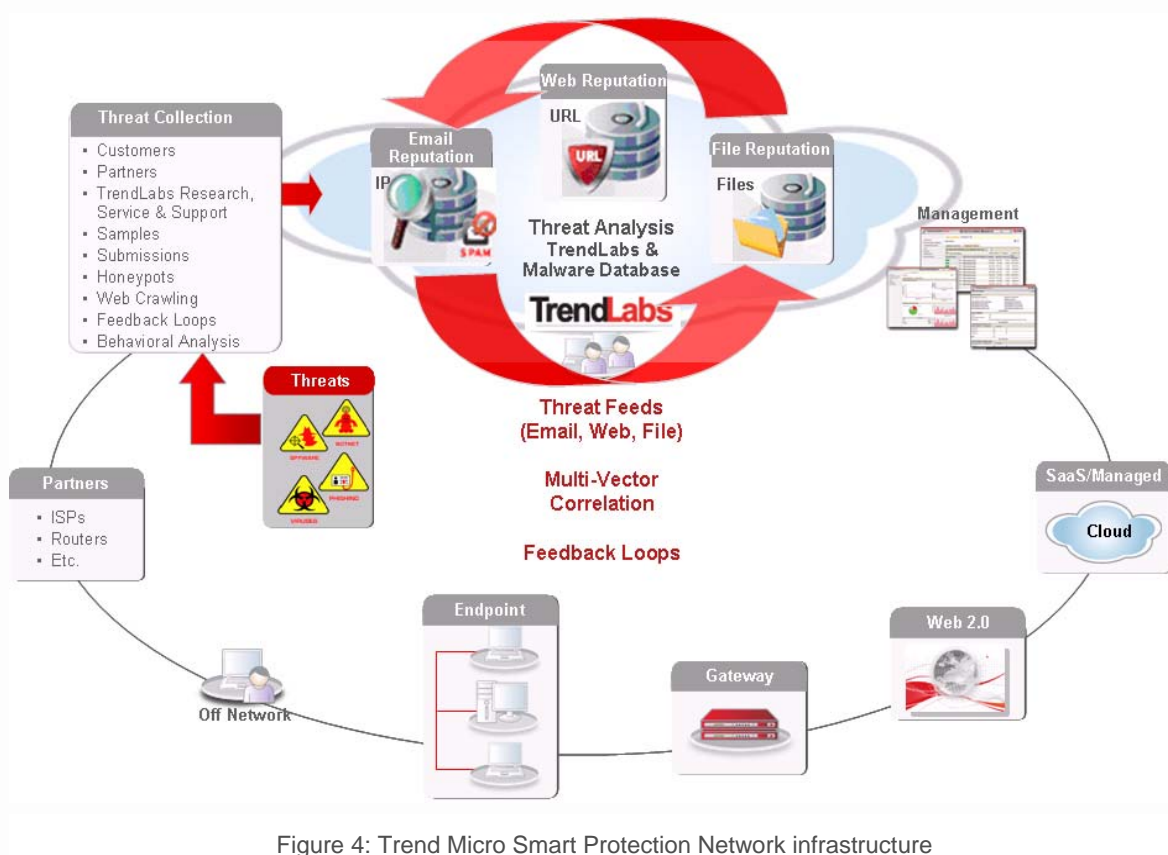


Figure 4: Trend Micro Smart Protection Network infrastructure

Web Reputation Technology

As a critical element of the Trend Micro Smart Protection Network, Web reputation technology guards against Web-based threats before they endanger a network or a user's PC. By assigning a relative reputation score to domains and individual pages within these domains, Web reputation technology weighs several factors, including a Web site's age, any historical location changes, and other factors that might indicate suspicious behavior. The technology then advances this assessment through malware behavior analysis, monitoring network traffic to identify any malware activity originating from a domain. Trend Micro Web reputation technology also performs Web site content crawling and scanning to complement this analysis with a block list of known bad or infected sites. Access to malicious Web pages is then blocked based on domain reputation ratings. To reduce false positives and increase accuracy, Trend Micro's Web reputation technology assigns reputations to specific pages or links, rather than an entire site, as sometimes only portions of a legitimate site are hacked.

Email Reputation Technology

As an additional layer of protection, email reputation technology can stop up to 80 percent of email-based threats, including emails with links to dangerous Web sites, before these threats reach the network or the user's PC. Email reputation technology validates IP addresses—or computer addresses—against both a reputation database of known spam sources and a dynamic service that can assess email sender reputation in real time. Reputation ratings are further refined through continuous analysis of the IP addresses' behavior, scope of activity, and prior history. Malicious emails are blocked in the cloud based on the reputation of the sender's IP address, preventing threats such as botnets from reaching the network or the user's PC. The reputation status is continually updated to ensure that a good reputation is restored when infected bots are cleaned, resuming delivery of legitimate email.

File Reputation Technology

The Trend Micro Smart Protection Network leverages file reputation technology, in addition to Web and email reputation technologies. Cyber criminals frequently move individual files with malicious content from one Web site to another to avoid detection, making file reputation checking a critical element to security in a Web 2.0 world. File reputation capabilities also address the fact that a reputation may not yet be assessed for a Web site that contains a malicious file. In addition, any file attached to an email is checked for malware. Malware in email attachments, if installed, can access the Web as an implementation mechanism. Files should also be checked on the Web itself. File reputation technology essentially checks the reputation of a file against an extensive database before permitting the user to download it. To accomplish this, a data crawl of each file hosted on a Web page or attached to an email, as well as an assessment of each file's reputation, is performed to continuously update a database of file reputation in real time.

By 2009, Trend Micro plans to integrate new, cloud-client file reputation technology into the portfolio of endpoint security solutions, expanding on a commitment to move more security capabilities into the Internet cloud. The

The Botnet Threat

A significant threat to the Internet, *botnets* are large pools of compromised computers located in homes, schools, businesses, and governments around the world. Under the control of a hacker, commonly known as a botmaster, botnets are used to conduct various attacks, ranging from distributed denial-of-service (DDoS) attacks to email spamming, keylogging, click fraud, and malware distribution. Botnets may encompass thousands of compromised hosts, or bots, and can aggregate a tremendous amount of computing power to attack a wide range of targets. For instance, a botmaster can command each bot to launch spamming emails or steal credit card information from against thousands of computer hosts to maximize financial gains.

technology will become an integral part of the Trend Micro Smart Protection Network, providing fast, real-time security status “look-up” capabilities in the cloud and further reducing the cost and overhead associated with corporate-wide pattern deployments.

The Web, email, and file reputation databases in the cloud receive constant updates—leveraging patent-pending correlation technology and enabling Trend Micro to quickly respond to and remediate new Web and email threats.

Correlation Technology with Behavior Analysis

The Trend Micro Smart Protection Network uses “correlation technology” with behavioral analysis to correlate combinations of threat activities to determine if they are malicious. Although a single email or other component of a Web threat may appear innocuous, several activities used in conjunction can create a malicious result. So a holistic view—gained by examining the relationship between and across the different components of a potential threat—is required to determine if a threat is actually present.

For example, a user may receive an email from a sender whose IP address has not yet been identified as that of a spam sender. The email includes a URL to a legitimate Web site that is not yet listed as malicious in a Web reputation database. By clicking on the URL, the user is unknowingly redirected to a malicious Web site hosting “information stealers” that are downloaded and installed on the user’s computer, gathering private information for criminal purposes.

Behavior analysis also correlates activities of a single session on the same protocol (e.g. an SMTP attachment with a suspicious double extension), as well as activities during multiple network connection sessions on the same protocol (e.g. a downloader blended threat in which individual files that each appear to be innocent are downloaded, but together form a malicious program). In addition, activities of multiple sessions and different protocols (e.g. SMTP and HTTP) are correlated to identify suspicious combinations of activities (e.g. an email with a URL link to several recipients and an HTTP executable file download from the linked Web page).

Information learned in the behavior analysis function at the gateway is looped back to provide the Web reputation technology and database with site-threat correlation data and to update the email reputation database of known bad IPs and domains. Similarly, information acquired at the endpoint is looped back to the file scanning capability at the gateway, network servers, and the Web reputation capability in the cloud. Both feed-through and loop-back techniques are needed to ensure real-time, Web threat protection across the entire network.

Smart Protection—By the Numbers

- Trend Micro Smart Protection Network handles more than five billion URL, email, and file queries daily.
- Trend Micro processes more than 50 million IP addresses and URLs daily.
- More than 250 million sample submissions originate from Trend Micro’s comprehensive, global threat collection system of traps, honeypots, product feedback loops, and other proven collection techniques.
- Trend Micro maintains datacenters in five locations around the globe, processing more than 1.2 terabytes of data every day.
- Trend Micro has more than 1,000 security experts committed to constant global threat surveillance and attack prevention. Every day, Trend Micro breaks 8 to 10 million infections.

TREND MICRO™ SMART PROTECTION NETWORK— SECURITY MADE SMARTER.

By correlating different threat components and continuously updating its threat databases, Trend Micro has the distinct advantage of responding in real time, providing immediate and automatic protection from email and Web threats.

Feedback Loops

Additionally, because Trend Micro solutions act as a single, cohesive security platform, built-in feedback loops provide continuous communication between Trend Micro products and Trend Micro's threat research centers and technologies in a two-way update stream to ensure rapid and optimal protection against the latest threats.

Functioning like the "neighborhood watch" approach occurring in many communities, Trend Micro's extensive global feedback loop system contributes to a comprehensive, up-to-date threat index that enables real-time detection and immediate, "smarter together" protection. Each new threat identified via a single customer's routine reputation check, for example, automatically updates all Trend Micro's threat databases around the world, blocking any subsequent customer encounters of a given threat.

Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, latency is not an issue, and the privacy of a customer's personal or business information is always protected.

Threat Intelligence

Trend Micro supplements user feedback and submissions with internal research culled from researchers in the United States, the Philippines, Japan, France, Germany, and China. Multilingual staff members at TrendLabs—Trend Micro's global network of research, service and support centers—respond in real time, providing 24/7 threat surveillance and attack prevention to detect, pre-empt, and eliminate attacks.

Using a combination of technologies and data collection methods—including "honeypots," Web crawlers, customer and partner submissions, feedback loops, and TrendLabs threat research—Trend Micro proactively gains intelligence about the latest threats. This threat data is analyzed and correlated in real time via queries of Trend Micro's malware knowledge databases in the Internet cloud and by TrendLabs research, service, and support centers.



V. CASE STUDY—THE BRAZILIAN TAX SCAM

The Problem

Today's threats are growing increasingly sophisticated and challenging to combat. For example, a group of cyber criminals recently took advantage of the Brazilian tax season by spamming timely, tax-themed email messages that were actually phishing baits. The criminals used logos of the agencies being spoofed, tricking taxpayers into falling for the scams.

In this particular example, Brazilian taxpayers received a spammed email message that appeared to come from the Ministry of Finance and asked recipients to confirm that their income tax return had not yet been delivered. Users who clicked on any of the links inside the email were led via a legitimate Web site address to a malicious URL hijacked by the cyber criminals, which prompted a file download. The URL also pointed to several other malware hosted on the site. The malicious files were variants of a malware family notorious for downloading information stealers onto computers.

Information stealers gather a variety of user information such as account login credentials, details of online transactions, computer system information, and serial numbers of legitimate installed software, as well as user browsing habits.



Figure 5: A phishing email purporting to come from the Ministerio de Fazenda

In the case of the Brazilian tax threat, the spyware sent taxpayer information to a predetermined email address—unbeknownst to the user. Once installed on the user's computer, the malware continually downloaded new components, changing its shape and nature to evade conventional security protection.

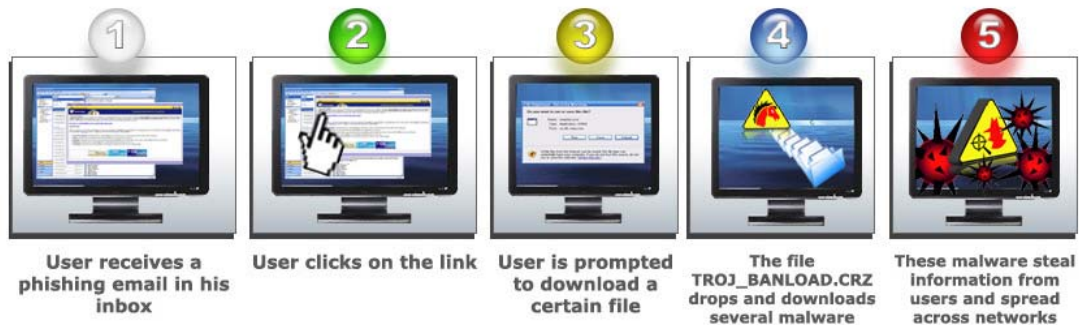


Figure 6: The Brazilian tax scam threat sequence

The Solution

First, the Trend Micro Smart Protection Network intercepts the email and checks the IP address, or computer address, of the sender against Trend Micro's email reputation database. If the IP address is identified as that of a spam sender, the email is blocked.

Next, the Web link embedded in the email is extracted and checked against Trend Micro's Web reputation database to ensure the user is blocked from accessing malicious Web sites. In addition, components hosted on the Web site are automatically downloaded and analyzed. Files found are checked against Trend's threat databases in the cloud.

All the content inside each embedded Web object is also analyzed because these objects can contain lists of IP addresses that link back to additional, potentially malicious components. The results are immediately added to all of Trend Micro's interconnected, Internet-based threat databases. All of these activities occur in the Internet cloud, before threats can reach an organization's network or a PC—providing a web of protection to secure a company's information and reputation.

Threats such as the Brazilian tax scam frequently include a variety of different components that may each appear benign but in combination result in a malicious, coordinated attack. The Trend Micro Smart Protection Network leverages patent-pending technology to correlate all of the threat data collected and protect against coordinated attacks in real time.

Cyber criminals are becoming more sophisticated every day. Backed by 20 years of leadership in Internet content security and more than 1,000 security experts worldwide providing 24/7 threat surveillance and attack prevention, Trend Micro delivers a smarter approach to security with the Trend Micro Smart Protection Network.



VI. CONCLUSION

In the past, Web threats were fewer and more static. This enabled manageable pattern file deployments to provide protection. Today, however, thousands of daily threats change rapidly and use multiple modalities to circumvent the best security efforts, while stealing confidential information from consumers and enterprises alike. The result is a dramatic increase in the number of pattern file downloads and a significant impact on network bandwidth and system resources.

The Trend Micro Smart Protection Network is a next generation, cloud-client content security infrastructure designed to protect users from Web threats while reducing the network and system impact, and the reliance on conventional pattern file downloads.

Leveraging both internal expertise in delivering leading content security solutions and real-time feedback from customer environments, the Trend Micro Smart Protection Network correlates information from multiple vectors to deliver comprehensive Web threat protection. The Trend Micro Smart Protection Network is used in on-site and hosted Web, messaging, and endpoint security solutions to protect companies and end-users from threats that compromise information and severely damage a company's or an individual's reputation.

VII. ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide. Please visit www.trendmicro.com.

Copyright© 2008 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



REFERENCES

- ¹ ConsumersUnion.org, “U.S. Consumers Lose More Than \$7 Billion to Online Threats,” Consumer Reports,” <https://secure.consumersunion.org/site/Advocacy?JServSessionIdr007=jkjuzxl2t1.app43a&cmd=display&page=UserAction&id=1799>, August 6, 2007.
- ² Center for Identity Management and Information Protection (CIMIP) at Utica College, NY, “Identity Fraud Trends & Patterns,” <http://ww.utica.edu/academic/institutes/cimip/publications/index.cfm>, October 2007.
- ³ Ross Kerber, “Cost of data breach at TJX soars to \$256m,” Boston Globe, http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/, August 15, 2007.
- ⁴ Ponemon Institute, “2007 Annual Study: U.S. Cost of a Data Breach,” http://www.ponemon.org/press/pr_ponemon_2007-cob_071126_f.pdf, November 28, 2007.
- ⁵ Marius Oiaga, Softpedia, “Hacking Russian Trio Gets 24 Years in Prison,” <http://news.softpedia.com/news/hacking-russian-trio-gets-24-years-in-prison-37149.shtml>, October 4, 2006.
- ⁶ Byron Acohido and Jon Swartz, USA TODAY “Cybercrime flourishes in online hacker forums,” http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hackerforums_x.htm, October 11, 2006.
- ⁷ Gregg Keizer, TechWeb Technology News, “Botnet Creator Pleads Guilty, Faces 25 Years,” <http://www.techweb.com/wire/security/177103378>, January 24, 2006.
- ⁸ AV-Test GmbH, www.av-test.org.

