TREND MICRO

Trend Micro™
Smart Protection Network™
Security Made Smarter

→Core Technology

A Trend Micro White Paper | June 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the underground economy has grown and prospered, cybercriminals have developed increasingly sophisticated malware as tools of their trade. Yet, as these criminals prosper, businesses and consumers alike are suffering data leakage, 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 antivirus protection is falling short and security update deployment issues are impacting network and system performance.

Trend Micro offers a new approach to combat evolving threats with the Trend Micro™ Smart Protection Network™—a next-generation, cloud-client, content security infrastructure designed to protect against today's threats. The 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 threat data gathered through a network of proactive email, web, and file reputation technologies, web crawlers, honeypots, and global threat sensors. This data is collected from customers, partners, and research and support centers to combat sophisticated sequential and blended threats. Built-in smart feedback and communication between Trend Micro's 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 the dangerous world of cybercrime and outlines the challenges that security professionals face in developing solutions to address the growing number and variety of threats. Finally, this paper explores how the Smart Protection Network can deliver next-generation security to automatically protect digital information wherever users connect.

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 cybercriminals lurk behind most threats today, creating a new generation of malware that drives a powerful underground economy.

According to the 2009 Internet Crime report, 336,655 total complaints were filed with the Internet Crime Complaint Center (IC3), representing a 22.3 percent increase compared to 2008 and a 62.7 percent increase since 2007. In addition, the total dollar loss from all referred cases was $559.7 million—up from $264.6 million in total reported losses in 2008.[1]

In 2009, identity theft ranked as the number-one consumer complaint category with 1.3 million people falling victim to the crime, or 21 percent of all complaints, according to the Federal Trade Commission (FTC).[2] Businesses also suffer from the effect of cybercrime. For example, the recent large-scale data breach involving Heartland Payment Systems, one of the five largest payment processors in the U.S., occurred when cybercriminals managed to sneak a keystroke logger onto the company's credit card processing system. The stolen data included names,

credit and debit card numbers, and the expiration dates of credit and debit cardholders. Heartland serves 250,000 restaurants, retailers, and other businesses and conducts more than four billion business transactions per year.[3]

Consequences of data leaks are dire as corporations pay out millions of dollars in class-action lawsuits filed by the consumers whose data has been stolen. Heartland Payment Systems agreed to pay $41.4 million to eligible MasterCard issuers with respect to losses alleged to have been incurred by them as a result of the 2009 attack.[4] Companies also suffer from a loss in market share, falling stock prices, and a tarnished brand image.

Malware clean-up presents additional, costly challenges. In some cases, threats may cause 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 fail. Infected systems often require an expensive and complete system recovery, in which the operating system, applications, and user data must be reinstalled.

Internal 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, cybercriminals 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 fifth annual "U.S. Cost of a Data Breach Study," sponsored by the Ponemon Institute, data breach incidents cost U.S. companies $204 per compromised customer record in 2009 with average total per-incident costs in 2009 totaling $6.75 million. The most expensive data breach event included in the 2009 study cost nearly $31 million to resolve.[5] Additionally, each year companies incur billions of dollars in intellectual property losses to software, hardware design, drug formulations, and other trade secrets that are leaked.

The underground economy continues to flourish, and cybercriminals profit handsomely. For example, Trend Micro security researchers documented an affiliate who generated $300,000 from rogue antivirus installations in only one month. 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. For example, the recent takedown of Mariposa—one of the world's largest botnets—revealed the botnet had infected and controlled up to 12.7m PCs in 190 countries. Infected PCs were tracked back to US Fortune 1,000 companies and major banks, allowing botnet operators to steal credit card data, online banking credentials, and other sensitive data. Bank records and seized computers are still being examined to determine how much money the criminals made but experts theorize it will be a huge sum of money.[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 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 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. Today's threats directly impact businesses causing downtime, lost data, infections, reduced employee productivity, and time-consuming incident cleanup. Consumers suffer too—from stolen bank information and the costly consequences of identity theft, as well as from system slowdowns associated with compromised machines. As the digital underground economy grows more profitable, cybercriminals will continue to develop malware for profit, creating a critical need for adaptable security techniques and technologies that deliver better protection for all users.

THE CHANGING THREAT LANDSCAPE—SECURITY CHALLENGES

Combined Threats

Today's threats frequently combine a number of seemingly innocent programs to create an infection chain. For example, individual downloader programs, commonly used as a part of 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. Threats often expand this technique to include multilayered, multiprotocol coordinated attacks to avoid detection by conventional means.

For instance, a cybercriminal embeds a URL in an email or instant message. The user clicks on the link leading to a legitimate URL that was hijacked for a few days or hours. An ActiveX control then tests the user's browser vulnerability. If a vulnerability is detected, the malware attacks. If not, it downloads a file, tests for another vulnerability, downloads more files, and so on. Each session appears benign, but the combined activities represent a coordinated attack. A single security solution is no longer comprehensive enough to cover all aspects of these threats. As a result, information security today has reached a critical turning point—a new approach is needed to address today's highly sophisticated, sequential, blended threats.

Explosion of Web Threats

Historically, cybercriminals 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 in 2010, 1.5 million unique samples were reported per month.[8] See Figure 1.
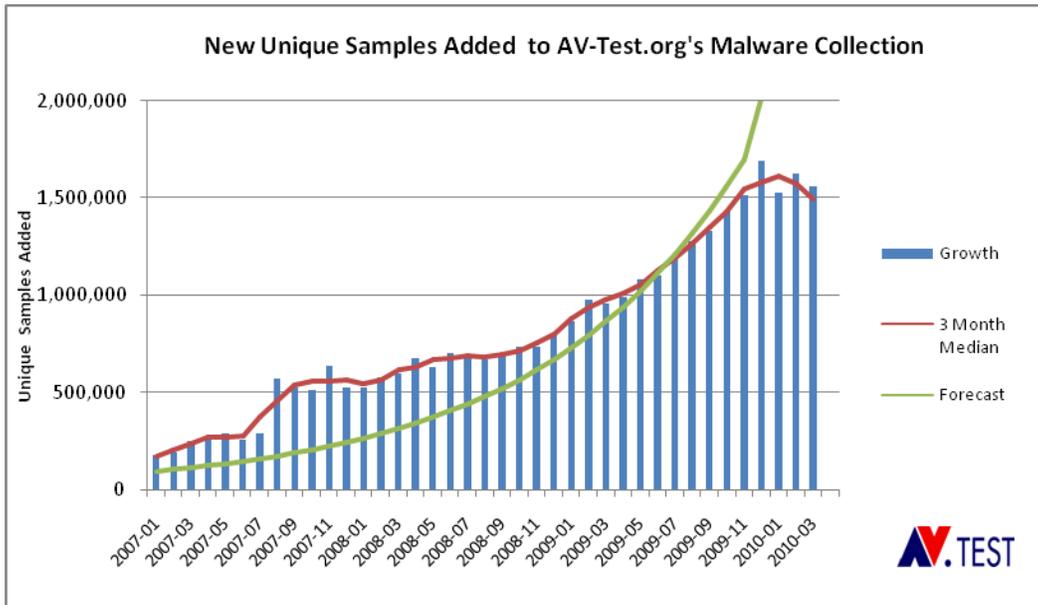

Figure 1: AV-Test.org reporting 1.5 million unique malware samples per month

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, evolve from the same piece of code. See Figure 2. Cybercriminals are fully aware of the difficulty in issuing updates, and they use this fact to their advantage, creating new malware quickly and en masse. Cybercriminals leverage services whereby they can test threats (URLs, domains, files) against most security vendor's protection options, allowing new threats to be published that evade the security industry.
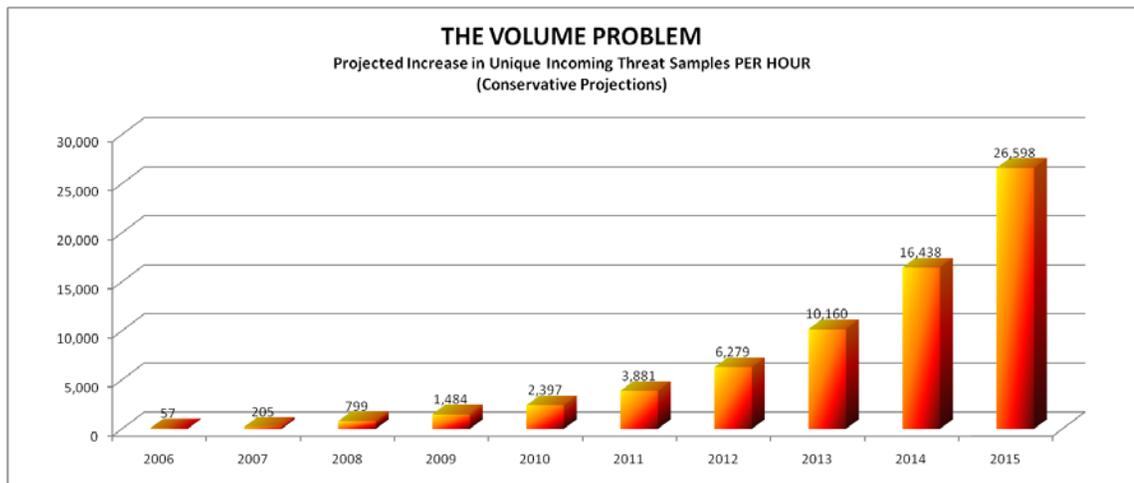

Figure 2: The volume problem

THE CONVENTIONAL APPROACH—PATTERN-BASED SOLUTIONS

Conventional malware protection involves gathering malware samples, developing patterns, and then quickly distributing these patterns to users. Because many threats encompass targeted, combined attacks, collecting samples is becoming 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 threats. Viruses were originally designed to spread as quickly as possible and were therefore easy to spot. With the advent of web-based threats, malware has evolved from an outbreak model to stealthy "sleeper" infections that are tougher to detect using conventional techniques.

Deployment Issues

The security industry reacted to the increasing number of malware by issuing more frequent updates. Some vendors switched from weekly to daily updates or updates every five minutes. The consequent update volume has significantly impacted the system and network resources required to manage pattern downloads, 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 the latest 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.

A NEW APPROACH—TREND MICRO SMART PROTECTION NETWORK

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

The Smart Protection Network infrastructure provides innovative, real-time protection from the cloud, blocking threats before they reach a user's PC or a company's network. Leveraged across Trend Micro's solutions and services, the 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 Smart Protection Network is composed of a global network of threat intelligence technologies and sensors that deliver comprehensive protection against all types of threats—

malicious files, spam, phishing, web threats, denial of service attacks, web vulnerabilities, and even data loss. By incorporating in-the-cloud reputation and patent-pending correlation technologies, the 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.

As shown in Figure 3, the Trend Micro Smart Protection Network includes the following components:

- Web Reputation technology
- Email Reputation technology
- File Reputation technology
- Correlation Technology
- Smart Feedback
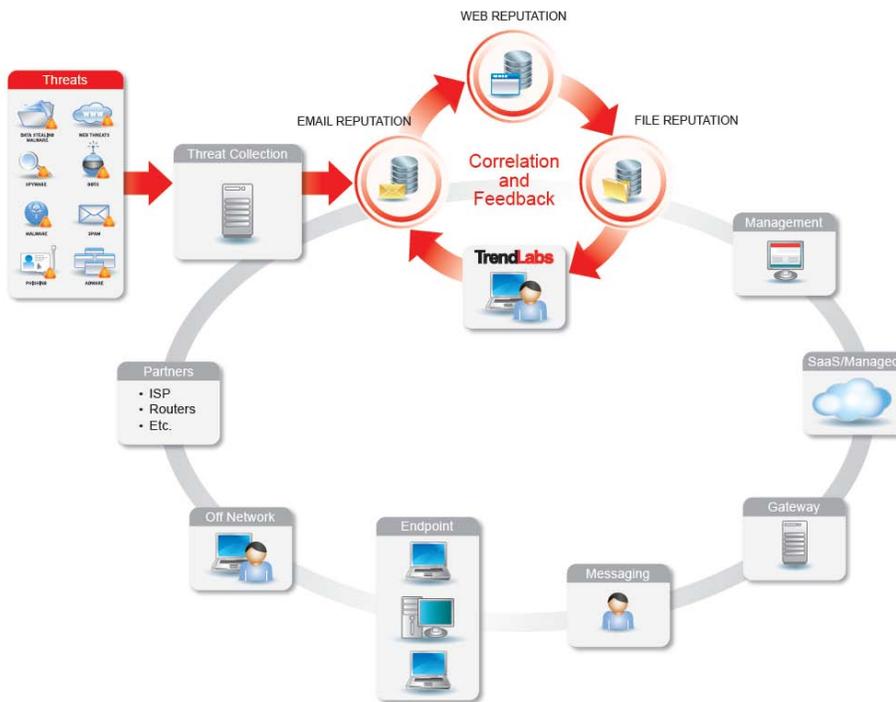- Threat intelligence (threat collection, threat analysis)

Figure 3: Smart Protection Network
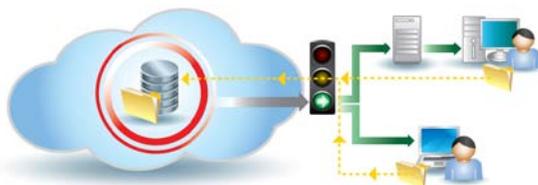
Web Reputation Technology

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 aggregated 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 blocks 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.

Traditional malware scanning identifies infected files by comparing several hash values of the file content with a list of hash values stored in a pattern or signature file. If a file is marked "suspect" in the first pass of hash comparison, the scan engine employs a multi-phase approach to further drill down. In all today's conventional endpoint security solutions, this pattern file is located on the endpoint and has to be distributed regularly to provide protection against the latest threats.

Trend Micro breaks that paradigm with File Reputation technology that decouples the pattern file from the local scan engine and conducts pattern file lookups over the network to a Smart Protection server. The Smart Protection server may reside on the customer premises (private cloud) or even on the Internet (public cloud). This in-the-cloud approach alleviates the challenge of deploying a large number of pattern files to hundreds or thousands of endpoints. With Trend Micro's new approach, as soon as the pattern is updated on the Smart Protection server, protection is immediately available to all clients leveraging that scan server. File Reputation addresses today's endpoint security challenges by providing shorter time to protect while assuring less complexity.

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, email, and file-based threats.

Smart Protection—By the Numbers

- Smart Protection Network handles more than 45 billion URL, email, and file queries daily.

- Smart Protection Network blocks over 5 billion threats per day.

- Trend Micro maintains datacenters in five locations around the globe, processing more than 2.8 terabytes of data every day.

- Trend Micro has more than 1,000 security experts committed to constant global threat surveillance and attack prevention.

Correlation Technology
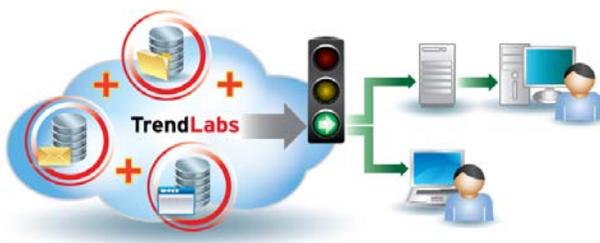
The Trend Micro Smart Protection Network uses patent-pending Correlation Technology with behavioral analysis to correlate combinations of threat activities to determine if they are malicious. Although a single email or other threat component may appear innocuous, several activities used in conjunction 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, threat protection across the entire network.

By correlating different threat components and continuously updating its threat databases, Trend Micro can respond in real time, providing immediate and automatic protection from file, email, and web threats. In the above example, Trend Micro analyzes the files being downloaded and determines they are malicious; therefore the files are added to the File Reputation database. If the IP where the spam originated is determined to be malicious, it is added to the Email Reputation database and the URL from the malicious website is added to the Web Reputation database to protect users from accessing that page. From that point on, all Trend Micro's customers will be protected if they access any of the three vectors involved in the threat—email, web, or file.

Smart Feedback

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

Functioning like the "neighborhood watch" approach occurring in many communities, Trend Micro's extensive global feedback 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 subsequent 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 smart feedback and submissions with internal research culled from researchers in the United States, South America, 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 gathers 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.

CASE STUDY—THE PERSISTENT ZEUS THREAT

The Problem

Created by Eastern European organized criminals, ZeuS is primarily a crimeware tool designed to steal money. Also known as ZBOT due to its botnet capabilities, ZBOT Trojans execute information-stealing routines that specifically target users' banking credentials. Reports show that the malware commonly hides behind the guise of a courier invoice or a security update.

ZeuS uses a complex encryption technique and features three, main components, including:

1. ZeuS Trojan

2. ZeuS configuration file (*config*)

3. ZeuS drop zone where stolen credentials are sent

After execution, the ZeuS Trojan downloads its configuration file from a predetermined location then waits for the victim to log in to a particular target that its *config* file has defined—usually a selection of banks and their login URLs.

Unlike traditional keyloggers, ZeuS Trojans are "men-in-the-browser" agents that grab variables from a browser session such as an online banking session. ZeuS is especially dangerous because it can also inject additional form fields into a legitimate web session. Injecting additional fields can urge victims to surrender more information than they would normally, for instance, with banks.

Some ZeuS variants also contain a nasty feature called "JabberZeuS," which immediately relays victims' login credentials to cybercriminals in real time via instant messaging. This allows cybercriminals to bypass multifactor authentication schemes to log in to victims' accounts and wire money to third parties, virtually piggybacking on the victims' sessions. This is where the ZeuS botnet's real power lies—the core nature of which is wholesale theft.

> The ZeuS Trojan originated several years ago, however, it has been rampantly used in the past year. In the past four months Trend Micro has identified an average of around 300 unique ZeuS samples per day. In fact, there were more than 13,000 unique ZeuS samples in January 2010 alone.

Part of ZeuS' success lies in file compression software that can encrypt application code, making it difficult to analyze. Also, ZBOT variants perform several stealth routines in order to hide themselves from users.

Like many of today's threats, ZeuS uses targeted, timely social-engineering ploys to enter victims' PCs. From banks and social-networking sites to patch updates and pop star news, ZeuS uses a variety of scams to bait users and steal money. ZeuS is best known for its information-stealing routines, which are created using toolkits that allow remote control of the malware. Getting the malware to infect target systems is the tricky part. ZeuS authors have tried using drive-by downloads, spammed messages, worm propagation, file infection, and other ways.

The malware detected by Trend Micro as PE_ZBOT.A injects code into target files and modifies its entry point to redirect to its code. This allows the malware to run code whenever the infected file is executed. It then attempts to connect to the remote sites from which it downloads and executes malicious files that steal information from an affected system. The downloaded files are detected as TROJ_KRAP.SMDA and TSPY_ZBOT.SMAP. Once the routine is complete, ZeuS returns control of the affected system to its host file.

The Solution

The Trend Micro Smart Protection Network protects users from ZeuS-related attacks by detecting and preventing PE_ZBOT.A and TROJ_KRAP.SMDA from executing on systems via the file reputation service.

The Smart Protection Network also intercepts 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 ZeuS spam sender, the email is blocked.

Web links embedded in spam are 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.

The content inside each embedded web object is also analyzed to see if it contains lists of IP addresses that link back to additional, potentially malicious components. The results are immediately added to Trend Micro's interconnected, Internet-based, threat databases. All these activities occur in the Internet cloud, before ZeuS 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 Zeus botnet frequently include a variety of 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 the threat data collected to protect against coordinated attacks in real time.

Cybercriminals are becoming more sophisticated every day. However, backed by 20 years of leadership in Internet content security, more than 1,000 global security experts delivering 24/7 threat surveillance and prevention, and the Smart Protection Network, Trend Micro delivers a smarter approach to beating cybercrime.

CONCLUSION

In the past, threats were fewer and more static. This enabled manageable pattern file deployments to provide protection. Today, however, thousands of daily threats using multiple modalities are circumventing even the best security efforts resulting in loss of confidential consumer and business information. 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 threats while reducing network and system impact, and reliance on conventional pattern file downloads.

Leveraging both internal expertise in delivering leading content security solutions and real-time feedback from customer environments, the Smart Protection Network correlates information from multiple vectors to deliver comprehensive threat protection. The 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 reputation or an individual's identity.

ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in Internet content security and threat management, aims to create a world safe for the exchange of digital information for businesses and consumers. A pioneer in server-based antivirus with over 20 years experience, we deliver top-ranked security that fits our customers' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology and products stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

Please visit www.trendmicro.com.

Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Endnotes

1 "2009 Internet Crime Report," IC3 web site, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

2 Garrett Godwin, "2010 FTC Identity Theft Statistics," Examiner.com, March 5, 2010, http://www.examiner.com/x-15313-Detroit-Pop-Culture-Examiner~y2010m3d5-2010-FTC-Identity-Theft-Statistics?cid=exrss-Detroit-Pop-Culture-Examiner

3 Richard Adhikari, "Cyber Thieves Hit Payment Processor Heartland," InternetNews.com, January 21, 2009, http://www.internetnews.com/security/article.php/3797551

4 "Heartland Payment Systems® and MasterCard Agree to $41.4 Million Intrusion Settlement," press release on Heartlandpaymentsystems.com web site, May 19, 2010, http://www.heartlandpaymentsystems.com/article/Heartland-Payment-Systems-and-Mastercard-Ag-6349.aspx

5 "Ponemon Study Shows the Cost of a Data Breach Continues to Increase," Press release on Ponemon.org, January 25, 2010, http://www.ponemon.org/news-2/23

6 Byron Acohido and Jon Swartz, "Cybercrime flourishes in online hacker forums," USA TODAY, October 11, 2006, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hackerforums_x.htm

7 Charles, Arthur, "Alleged controllers of 'Mariposa' botnet arrested in Spain, Guardian.co.uk, March 3, 2010, http://www.guardian.co.uk/technology/2010/mar/03/mariposa-botnet-spain

8 AV-Test GmbH, www.av-test.org.