TREND MICRO

Trend Micro Threat Discovery Service

Company X

Trend Micro Threat Discovery Service
Executive Summary Report

January 1, 2010 - January 31, 2010

Confidential

Highlights

BUSINESS RISKS

- High risk of Information Loss
- High risk of System Compromise
- High risk of Network Disruption
- High risk of Infection Spread

Overall Risk Level - High

AFFECTED ASSETS

- 28 endpoints are infected with malware
- 7 endpoints are running disruptive applications
- 25 of the infected endpoints are from Test

INFECTION SOURCES

- 958 malicious website visits
- 76 malware downloaded to the endpoints
- 0 malicious emails received

THREAT STATISTICS

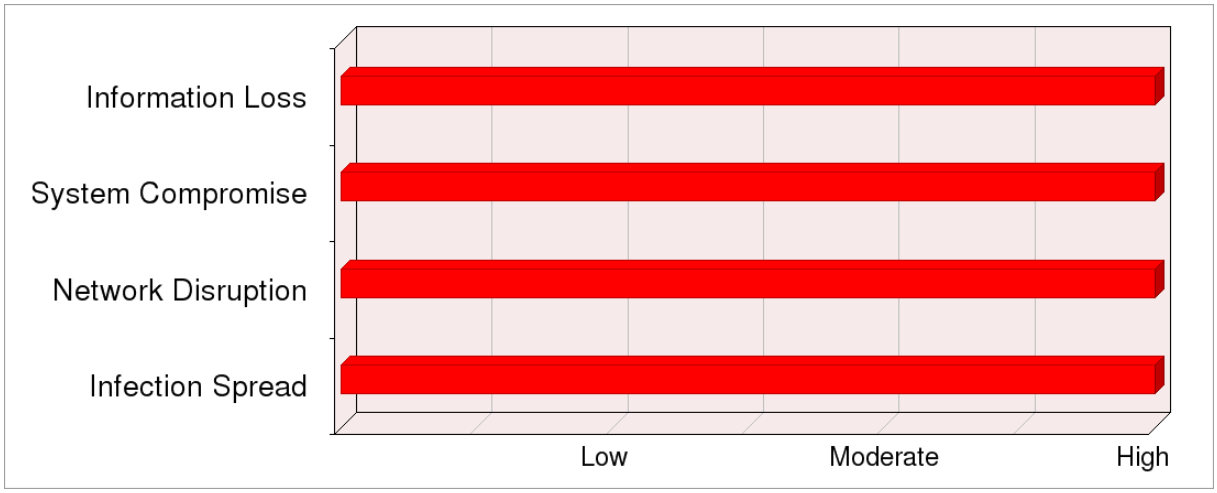
- 303 Generic Malware incidents have been detected
- 158 Data Stealing Malware incidents have been detected
- 149 IRC Bot incidents have been detected
- 665 threat incidents are detected from Test

POTENTIAL SECURITY RISKS

- 7 endpoints are running IM applications
- 0 endpoints are running peer - to - peer applications
- 0 documents were sent via potentially risky protocols

Business Risk Profile

These risk ratings are based on the threats detected by the Threat Discovery Appliance in your network for this reporting period



Risk of Information Loss -High

This is the risk that sensitive user and corporate data will be stolen and sent out to unauthorized external parties. Many malware have the ability to monitor the user's activities such as logging keystrokes or actively searching the endpoint for confidential documents to steal.The risk rating High is the average score for this reporting period.

Risk of System Compromise -High

This is the risk that unauthorized external parties will gain partial or complete control of your endpoints. Many malware such as IRC bots have the ability to connect to malicious servers in order to get commands external parties, essentially creating a backdoor to your network.The risk rating High is the average score for this reporting period.

Risk of Network Disruption -High

This is the risk that your network resources will be affected. Malware such as spambots and network worms often consume large amounts of network bandwidth thereby affecting overall network performance.The risk rating High is the average score for this reporting period.

Risk of Infection Spread -High

This is the risk that malware will propagate to other endpoints in your network. Malware such as network worms have the ability to locate and infect endpoints that have security vulnerabilities.The risk rating High is the average score for this reporting period.

Affected Assets

Affected Assets by Threat Type Summary

Affected assets results are based on the security incidents discovered by Threat Lifecycle Management Service in your network for this reporting period. The table below shows the total number of affected endpoints per threat type.

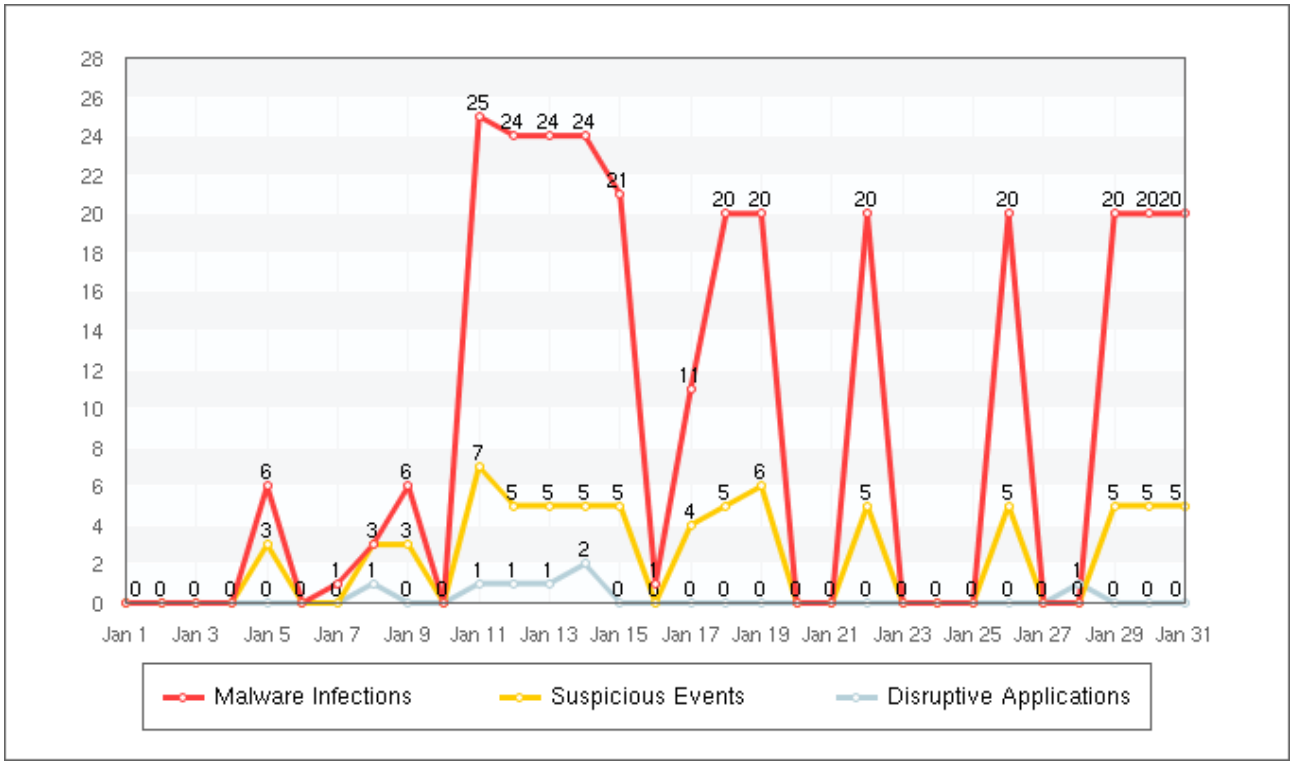
Affected Assets by Threat Type Summary			
Group	Threat Type		
	Malware Infections	Suspicious Events	Disruptive Applications
Test	25	8	7
George	1	1	0
Internal	3	0	0
TOTAL	**29**	**9**	**7**

Malware Infections - *endpoints that are confirmed to be infected with malware*

Suspicious Events - *endpoints that have been detected by TDA to have accessed malicious links, visited malicious websites or received malicious emails but show no signs of successful infection*

Disruptive Applications - *endpoints that are running disruptive applications such as IM & P2P*

Affected endpoints during the past 31 days



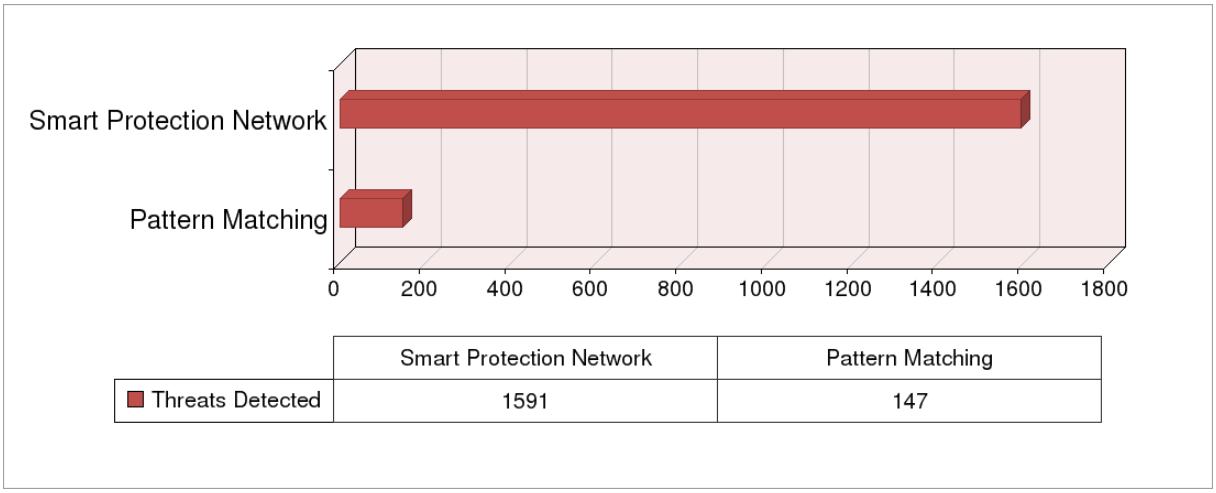
Infection Sources

Infection sources by threat infection behaviors

Infection Sources by Threat Infection Behaviors / Group			
Group	Threat Infection Behaviors		
	Visited Malicious Links	Downloaded Malware	Malicious Email
Test	956	75	0
George	2	1	0
Undefined*	0	0	0
TOTAL	**958**	**76**	**0**

Visited Malicious Links - *endpoints that have visited websites known by Trend Micro to be malicious*
Downloaded Malware - *endpoints that have downloaded files that are known to be malicious*
Malicious Email - *endpoints that have received emails with malicious links or attachments*
*Endpoints that do not belong to a defined monitored network

Detection Technology Used



Threat Statistics

Threat Incident Summary by Group / Threat Type			
Group	Threat Type		
	Generic Malware	Data Stealing Malware	IRC Bot
Test	302	146	149
George	1	0	0
Internal	0	12	0
TOTAL	**303**	**158**	**149**

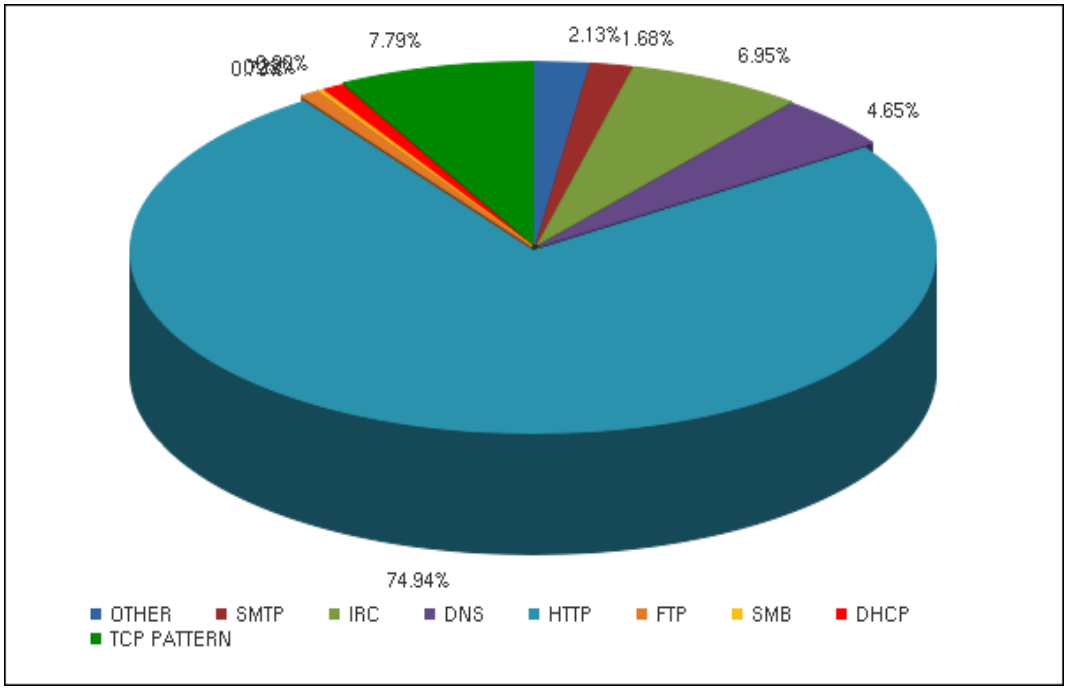
Generic Malware - *Any malicious software, including Viruses, Worms, Trojans, Password-stealers, Backdoors, and more.*

Data Stealing Malware - *Data stealing malware stays hidden on a victim's computer, silently stealing sensitive data such as keystrokes typed by the victim, account login details, personally identifiable data, documents stored on the computer, and more. This stolen data is sent back to a location accessible the attacker.*

IRC Bot - *An IRC Bot is malware that hides on a user's computer and awaits commands from its master which are sent via the chat protocol known as Internet Relay Chat (IRC).*

WARNING! *Data Stealing Malware might steal the personal information from the infected endpoint. It potentially against the privacy of personal information regulation in different countries, for example: California SB1386.*

Threat Protocol Distribution



Disruptive Applications

The following Disruptive Applications Summary table shows a list of clients that were detected using disruptive applications such as Instant Messaging, Video Streaming or Peer-to-Peer applications.

Disruptive Applications			
Group	Disruptive Application type		
	Streaming Media	Peer-to-peer	Instant Messaging
Test	0	0	7
TOTAL	**0**	**0**	**7**

Impact

Below is the list of the potential impact of the threats detected on your network:

- **Massive consumption of network bandwidth**

  Worms are a particularly invasive and fast spreading type of malware known to cause the following harm to networks:

  Excessive exploit attempts on hosts inside or outside of the network, which often results in massive consumption of network bandwidth and further propagation of the worm

  Sabotaging of hosts by creating additional administrative accounts, creating new shared folders, and interfering with the operation of security software, resulting in a weakening of overall network security

- **The versatility of modern malware**

  In today's threat landscape, malware is quite versatile and capable of performing many different malicious activities. Any of the following are possible and typical of an infected host:

  Downloading of other malicious components, such as bots or backdoor programs, which external parties can use to gain control of the hosts in your network

  Excessive spamming, exploit attempts on hosts inside or outside the network, and Denial of Service (DoS) attacks on hosts outside the network, which often results in massive consumption of network bandwidth and further propagation of the malware

  Sabotaging of hosts by creating additional administrative accounts, creating new shared folders, and interfering with the operation of security software, resulting in a weakening of overall network security

  Theft of confidential and critical customer and company data that may be exposed, utilized or sold to other criminals

  Sending massive amounts of unsolicited and sometimes fraudulent, malicious, and illegal email messages that may appear to originate from your domain, which can cause legitimate email sent from your network to be blocked by other mail servers with spam protection

Recommendations

These recommendations are based on the threats detected by Threat Discovery Service in your network for this reporting period

- **OS patching and user education**

  Worms have been detected propagating in your network. Worms are able to successfully propagate when hosts on your network have weak passwords or lack the latest OS and service patches. Outbreaks can be prevented by keeping hosts on the network up to date with the latest Windows Updates and ensuring the use of strong passwords.

  It is also recommended that you educate your users on how malware can arrive in their system. Simply clicking on a malicious URL found in an email, web page, or instant message will open the browser to a web page that can automatically install the malware on his system if the browser is vulnerable. They typically use social engineering to entice, intimidate, or otherwise trick the victim into running malicious code or clicking on a URL.

- **Deploy additional security measures at your Internet Gateway**

  Numerous hosts in your network have been infected with malware.

  We recommend that you deploy additional security measures at your Internet Gateway. Due to the fast-evolving nature of these threats and the ever increasing number of legitimate websites being compromised to host malware, a simple URL filtering system in the Internet Gateway is usually not enough. We recommend that you use a product that combines both URL reputation/filtering and antivirus scanning capability.

  It is also recommended that you educate your users on how malware can arrive in their system. Simply clicking on a malicious URL found in an email, web page, or instant message will open the browser to a web page that can automatically install the malware on his system if the browser is vulnerable. They typically use social engineering to entice, intimidate, or otherwise trick the victim into running malicious code or clicking on a URL.

  Automatic propagation via open vulnerable services or network shares is also possible which is why it is critically important to enforce strong, secure passwords and to always keep hosts on the network up to date with patches for their OS, browser, and other applications.

Appendix

Summary of most affected endpoints

This table shows the rating of threat incidents per endpoint that the Threat Lifecycle Management Service discovered in your network for this reporting period.

Most Affected Endpoint Summary			
Host Name	User Account	IP Address	Total Incident Count
172.16.1.2		172.16.1.2	181
192.168.248.128		192.168.248.128	35
7.7.7.199		7.7.7.199	33
192.168.140.129		192.168.140.129	30
7.7.7.109		7.7.7.109	24
192.168.2.6		192.168.2.6	24
192.168.1.168		192.168.1.168	22
172.16.1.1		172.16.1.1	20
22.22.22.15		22.22.22.15	17
172.16.0.189		172.16.0.189	15
33.33.33.129		33.33.33.129	15
192.168.0.183		192.168.0.183	14
33.33.33.2		33.33.33.2	13
192.168.101.43		192.168.101.43	13
192.168.220.1		192.168.220.1	13
172.16.252.129		172.16.252.129	13
10.1.1.1		10.1.1.1	12
7.7.7.1		7.7.7.1	12
10.2.168.5		10.2.168.5	12
192.168.190.1		192.168.190.1	12

Glossary

Data Stealing Malware

Data stealing malware stays hidden on a victim's computer, silently stealing sensitive data such as keystrokes typed by the victim, account login details, personally identifiable data, documents stored on the computer, and more. This stolen data is sent back to a location accessible the attacker.

Disruptive Applications (DAE)

Disruptive Applications detected by the Threat Discovery Appliance include instant messaging, streaming media, and peer to peer applications. These types of applications are considered to be disruptive because they slow down the network, are a security risk, and are generally a distraction to employees.

Downloader

A downloader is a type of malware designed to download other malware. This is usually the first malware executed on a victim's computer, which then receives a list of URLs from some predetermined location, often somewhere on the internet controlled by the attacker, where it will download other malware. Downloaders are designed for flexibility for the attacker. They allow the attacker to easily make updates and changes.

Email Worm

An email worm is a type of malware that attempts to propagate by sending emails with malicious code, usually a copy of itself, as an attachment to a set of email addresses usually found on the victim's computer in an attempt to dupe the reader into running the attachment. In addition to propagation, email worms can perform other malicious activities on infected hosts.

Informational Incidents

Informational incidents are low confidence incidents detected by the Threat Discovery Appliance. By themselves, there may not be a cause for alarm. But once correlated with others, these incidents may prove to be part of something more insidious.

Instant Messaging

A form of real time electronic communication between two devices over a network using typed text.

Internet Safety Tips

Most malware threats seen today will find their way onto the victim's computer using one of many different attack vectors and protocols. They typically use social engineering to entice, intimidate, or otherwise trick the victim into running malicious code or clicking on a URL. The malicious code can arrive as an attachment in an email, a file transfer request in an instant messaging application, transparently installed with other "free" software, or disguised as some other software, document, or media. Simply clicking on a malicious URL found in an email, web page, or instant message will open the browser to a web page that can automatically install the malware on his system if the browser is vulnerable. Malware is often disguised as desirable software the victim is interested in such as a "necessary" update in order to view a video online, a serial key generator, or free "cracked" copy of some popular software. Automatic propagation via open vulnerable services or network shares is also possible which is why it is critically important to enforce strong, secure passwords and to always keep hosts on the network up to date with patches for their OS, browser, and other applications. Strong passwords should contain upper case letters, lower case letters, digits, punctuation, and other symbols.

IRC Bot	An IRC Bot is malware that hides on a user's computer and awaits commands from its master which are sent via the chat protocol known as Internet Relay Chat (IRC).
Network Worm	A network worm is a type of malware that attempts to propagate by searching for and attacking other vulnerable computers. In addition to propagation, network worms can perform other malicious activities on infected hosts.
Public IRC Server Usage	Some IRC bots will communicate on IRC servers that are publicly accessible and used for many different purposes. These servers are typically legitimate and are unaware of this abuse.
Spam Bot	A spam bot is a type of malware that is designed to silently send spam emails from the victim's computer.
Streaming Media	In the scope of this report, streaming media refers to embedded videos on web sites such as youtube.com, cnn.com, hulu.com, etc.
Worm	A worm is a malicious program whose main function is to propagate itself to other computers. There is a variety of methods worms use to propagate, and the method(s) used is a defining factor. For instance, a worm which uses instant messenger programs to propagate is known as an IM worm.