



**TREND**  
MICRO™

**Threat Management Services**

# Company X

## Executive Summary

April 20 – 27, 2009



Securing Your Web World





Trend Micro™ Threat Management Services

# Security Threat Assessment Report

Do you want to know if malware has infiltrated your systems? If sensitive data is being lost? The true measure of your endpoint, web, and messaging security?

The Security Threat Assessment Report provides valuable and insightful visibility into the effectiveness and state of your current security infrastructure by uncovering both active and potential threats that are evading your existing security measures. The powerful report details are enabled by the Trend Micro Threat Discovery technology, a key component of Trend Micro Threat Management Services.

This sample report illustrates the unique and valuable insights provided by the Security Threat Assessment and the power of Trend Micro Threat Management Services to keep your network permanently secure. The report allows you to:

- **Examine** potential vectors of infection
- **Identify** malware, information stealers, affected assets, and infection sources
- **Uncover** sensitive data loss and regulatory compliance violations
- **Pinpoint** specific problem areas by IP address
- **Evaluate** the effectiveness of your existing security solutions
- **Understand** how threats occurred, where they entered your network, and how to fill your security gaps

These and other Trend Micro Threat Management Services reports are an example of the continuous value you gain by layering a network security overwatch service on top of your existing security infrastructure. With Threat Management Services customers gain increased threat security and awareness with 360° visibility of network-wide pain points and as well as infection containment and remediation services.

## THE NEED FOR MORE VISIBILITY INTO YOUR SECURITY POSTURE

After conducting over 100 enterprise security threat assessments worldwide with Threat Management Services, Trend Micro found:

- 100% of companies had active malware
- 56% of companies had information-stealing malware
- 72% of companies had one or more IRC bots
- 80% of companies had malware web downloads
- 42% of companies had one or more network worms

Source: Figures calculated from 130 global Security Threat Assessments through August 2009. Companies had an average of 7,484 employees and included representatives from the manufacturing, government, education, financial services, retail, and healthcare sectors.

To learn more about the Security Threat Assessment with Trend Micro Threat Management Services, contact your Trend Micro representative or obtain our contact details online at: <http://us.trendmicro.com/us/about-us/contact/index.html>



# Highlights

## BUSINESS RISKS

- **High** risk of Information Loss
- **High** risk of System Compromise
- **High** risk of Infection Spread



## DATA LOSS STATISTICS

- **7** incidents of data leakage (see appendix for more information)
- The following compliance regulations may have been violated:
  - **PCI, PII and SB-1386**

## AFFECTED ASSETS

- **7** endpoints are leaking confidential information
- **33** endpoints are infected with malware
- **404** endpoints are running disruptive applications
- **23** of the infected endpoints are from Department\_Y

## INFECTION SOURCES

- **1206** malicious website visits
- **153** malicious emails received
- **32** malware threats downloaded to endpoints

## MALWARE THREAT STATISTICS

- **12** endpoints are infected with network worms
- **9** endpoints are infected with IRC bot
- **7** endpoints are infected with Spam bots
- **5** endpoints are infected with Information Stealing malware

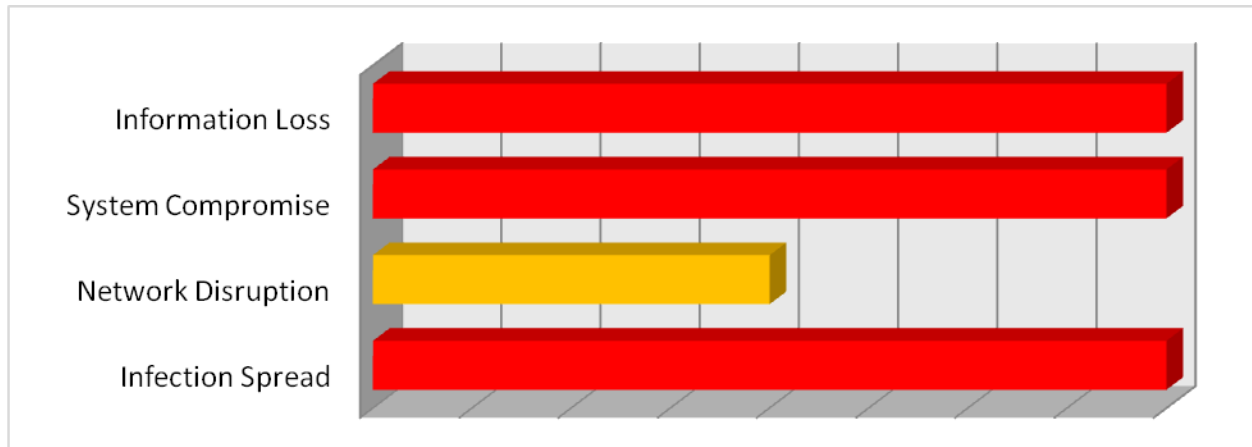
## POTENTIAL RISKS

- **358** endpoints are viewing streaming media
- **99** endpoints are running IM applications
- **1** endpoint is running peer-to-peer applications



# 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*

## 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 from external parties, essentially creating a backdoor to your network.*

## Risk of Network Disruption

**Moderate**

*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.*

## 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 or propagate through shared drives and folders.*



# Affected Assets

These results are based on the events detected by the Threat Discovery Appliance for this reporting period

Affected Endpoints			
Group	Incident Type		
	Malware Infections	Suspicious Events	Disruptive Applications
Department_Y	23	242	404
Undefined Group*	10	0	0
<b>TOTAL</b>	<b>33</b>	<b>242</b>	<b>404</b>

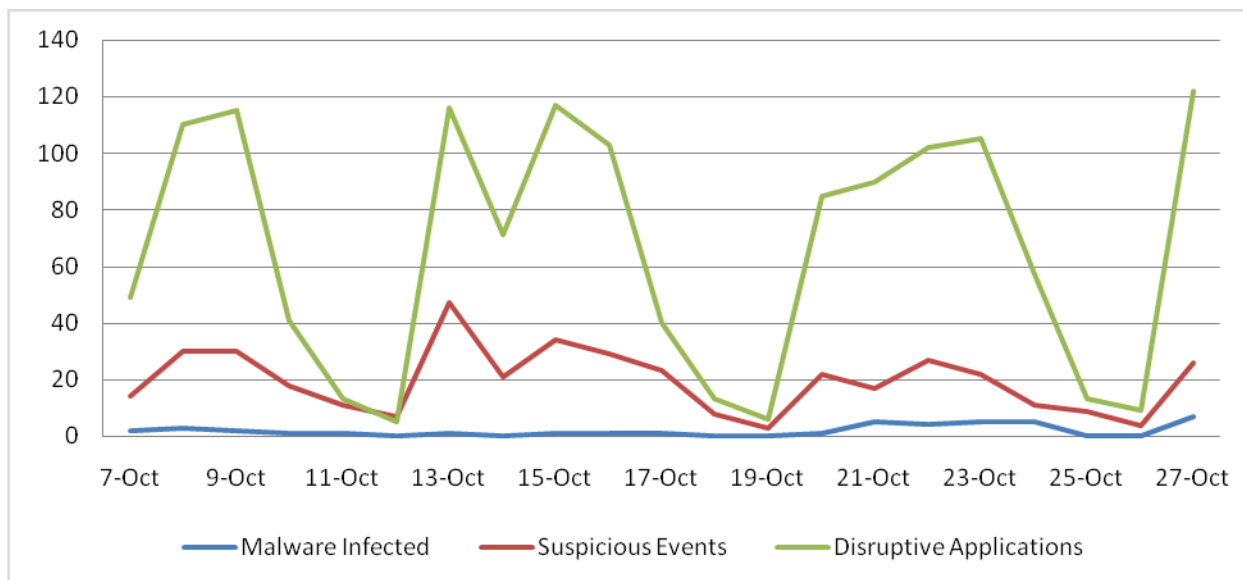
**Malware Infections** – endpoints that are confirmed to be infected with malware

**Suspicious Events** – endpoints that have been detected by TDA to have accessed malicious links, downloaded malware or received malicious emails

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

\*Endpoints that do not belong to a defined monitored network

## Affected endpoints for the past 22 days





# Infection Sources

These results are based on the events detected by the Threat Discovery Appliance for this reporting period

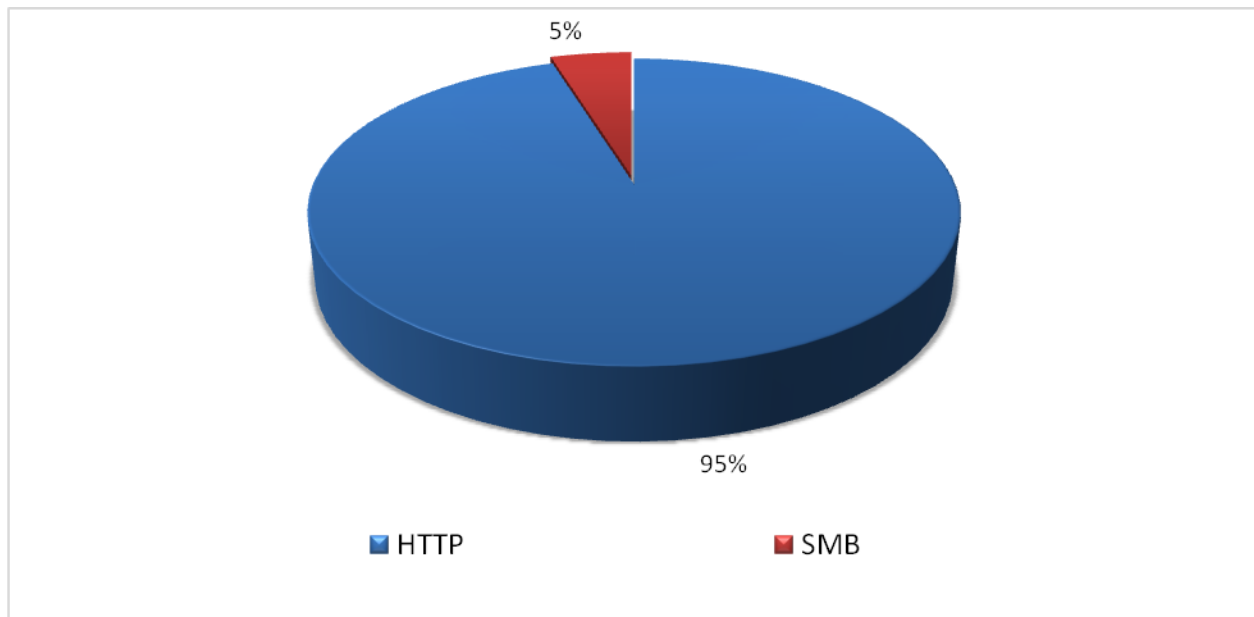
Potential Infection Sources			
Group	Incident Type		
	Malicious URL visits	Malware Downloaded	Malicious emails received
Department_Y	1206	32	153
<b>TOTAL</b>	<b>1206</b>	<b>32</b>	<b>153</b>

*Malicious URL visits* – total number of malicious URLs visited by endpoints

*Malware Downloaded* – total number of malware files downloaded files to endpoints

*Malicious emails received* – total number of malicious emails received by endpoints

## Threat Protocol Distribution





# Threat Statistics

These results are based on the events detected by the Threat Discovery Appliance for this reporting period

## Malware detected by TMS on endpoints

Group	Malware Type			
	Network Worm	IRC Bots	Spam bots	Information stealing malware
Department_Y	6	5	7	5
Undefined Group	6	4	0	0
<b>TOTAL</b>	<b>12</b>	<b>9</b>	<b>7</b>	<b>5</b>

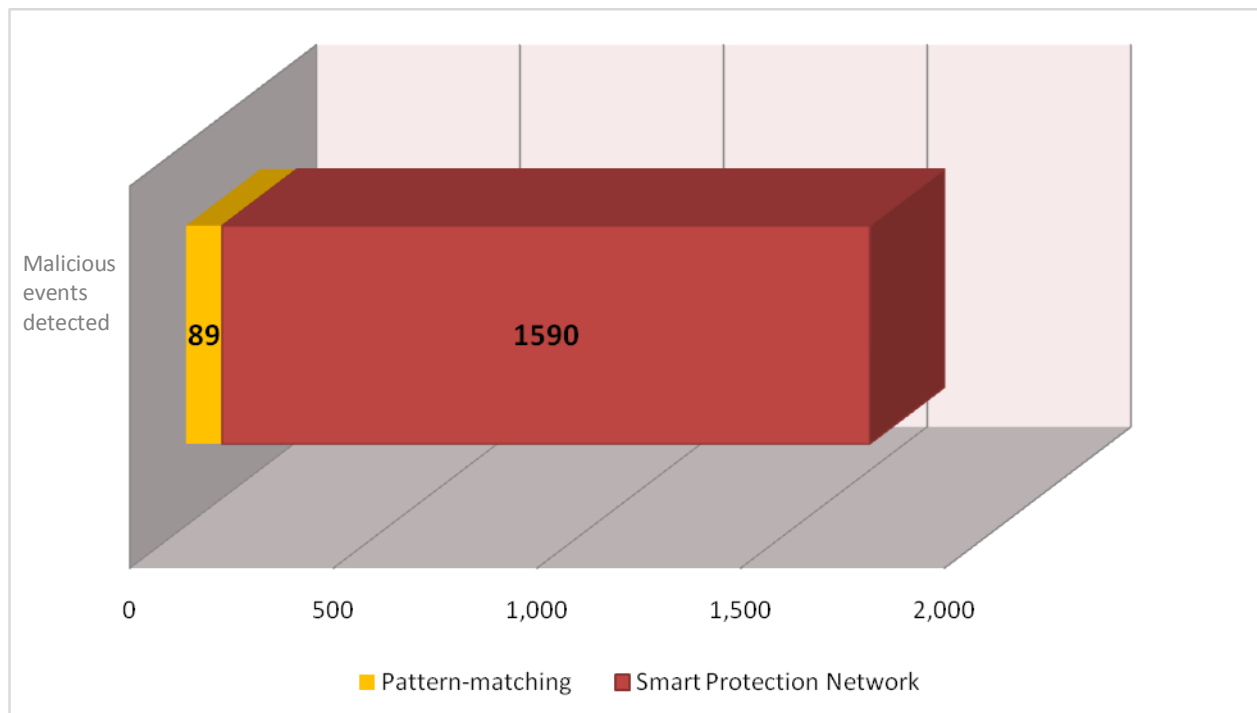
**Network Worms** – a type of malware that propagates by exploiting network vulnerabilities of hosts or propagates through shared drives or folders

**IRC Bots** – a type of malware that uses the Internet Relay Chat (IRC) protocol to connect to an external (C&C) server and receive instructions from its botmaster

**Spam Bot** - A spam bot is a type of malware that is designed to silently send spam emails from the victim's computer.

**Information stealing malware** - Information 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.

## Detection Technology Used





# Disruptive Applications

Potentially Disruptive Applications			
Group	Application Type*		
	Streaming Media	Peer-to-peer	Instant Messaging
Department_Y	358	1	99
<b>TOTAL</b>	<b>358</b>	<b>1</b>	<b>99</b>

\*further breakdown of the applications are available in the daily report

# Document Traffic Statistics

Outbound documents					
Filetype	Protocol				
	HTTP	FTP	SMTP	IM	Others*
Word	2225	235	0	0	5310
PPT	435	1	0	0	17
Excel	671	57	0	0	1460
Project	0	0	0	0	0
PDF	11796	869	0	0	3293

\*includes webmail



# Appendix

## List of endpoints leaking confidential information

IP Address	Hostname	Group	Timestamp	Regulations violated
10.2.8.9	cserver1.compx.com	Department_Y	4/27/2009 18:26	PCI, PII
10.65.210.30	9qkp9g1.compx.com	Department_Y	4/25/2009 08:31	PCI
10.65.90.180	38cy1.compx.com	Department_Y	4/24/2009 12:23	PCI
10.66.20.78	9grg1.compx.com	Department_Y	4/24/2009 07:33	PCI, PII, SB-1386
10.65.131.27	9x7m1.compx.com	Department_Y	4/23/2009 19:11	SB-1386
10.65.131.35	j7r71.compx.com	Department_Y	4/22/2009 23:33	SB-1386
10.65.132.190	9lj5d.compx.com	Department_Y	4/21/2009 19:55	SB-1386

## List of Infected Endpoints

IP Address	Hostname	Group	Threat Type	Details
10.2.8.9	Khy23a.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
10.3.210.27	ADPC1	Undefined_Group	Network Worm	WORM_MALAS.H
10.65.131.27	97m81.compx.com	Undefined_Group	Network Worm	VBS_RUNAUTO.M
10.65.131.35	j0tr7.compx.com	Undefined_Group	Network Worm	VBS_RUNAUTO.M
10.65.132.190	9lj51.compx.com	Undefined_Group	Network Worm	VBS_RUNAUTO.M
10.65.210.30	9qp91.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
10.65.90.180	30cyb.compx.com	Department_Y	Network Worm	VBS_RUNAUTO.M
10.66.20.78	9grb1.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
172.30.132.140	cyewpsf01.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
10.67.37.93	bvm3f1.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
10.66.64.82	dv5w1.compx.com	Undefined_Group	Network Worm	WORM_MALAS.H
10.65.80.129	4m8c1.compx.com	Department_Y	Network Worm	WORM_MALAS.H



10.65.80.156	xyza700ns571.compx.com	Department_Y	IRC Bot	us.magder.info
10.65.80.87	xy306t5c071.compx.com	Department_Y	IRC Bot	us.magder.info
10.65.80.129	4mc7c1.compx.com	Department_Y	IRC Bot	us.magder.info
10.65.80.135	xya27gg051.compx.com	Department_Y	IRC Bot	us.magder.info
10.65.80.66	xza24vfk1.compx.com	Department_Y	IRC Bot	us.magder.info

## Top endpoints that access malicious websites

*These endpoints constitute 80% of the total malicious website visits*

IP Address	Hostname	Group	Malicious URL visits
10.65.80.125	xyzg27063351.compx.com	Department_Y	113
10.65.110.96	xyza06czm7.compx.com	Department_Y	78
10.65.110.103	xzc30j3bw1.compx.com	Department_Y	73
10.65.70.99	xy70c8m71.compx.com	Department_Y	71
10.65.50.69	xz270fcp61.compx.com	Department_Y	61
10.65.70.126	btnxbox891.na.xom.com	Department_Y	58
10.65.80.228	lwg1.compx.com	Department_Y	39
10.65.100.87	Lwgs121.compx.com	Department_Y	36
10.65.80.239	fxkh1.compx.com	Department_Y	30
10.65.110.91	44r1.compx.com	Department_Y	29