



# Company X

## Executive Summary



Securing Your Web World



**CONFIDENTIAL**

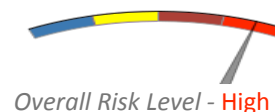


# Highlights

## BUSINESS RISKS

[Click on a line for details](#)

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



## AFFECTED ASSETS

[Click on a line for details](#)

- **61** endpoints are infected with malware
- **99** endpoints are running disruptive applications
- **61** of the infected endpoints are from the Department\_XXXX

## INFECTION SOURCES

[Click on a line for details](#)

- **24942** malicious website visits
- **346** malware downloaded to the endpoints
- **752** malicious emails received

## MALWARE THREAT STATISTICS

[Click on a line for details](#)

- **54** endpoints are infected with Generic malware
- **3** endpoints are infected with IRC bot
- **2** endpoints are infected with Information stealing malware
- **2** endpoints are infected with Spam Bot

## POTENTIAL SECURITY RISKS

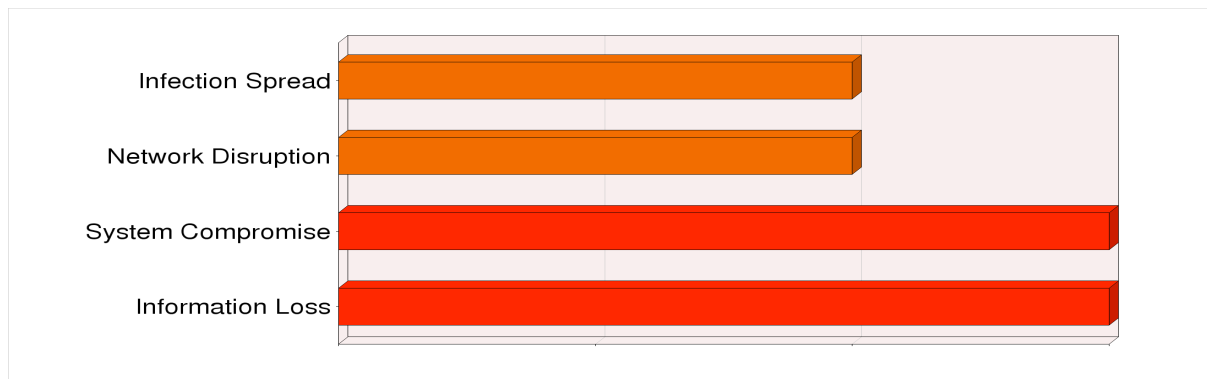
[Click on a line for details](#)

- **99** endpoints are running peer - to - peer applications
- **100550** 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.

## 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.

## 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

**Moderate**

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.



# 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_XXXX    | 61                 | 1560              | 99                      |
| Undefined Group*   | 0                  | 43                | 0                       |
| <b>TOTAL</b>       | <b>61</b>          | <b>1603</b>       | <b>99</b>               |

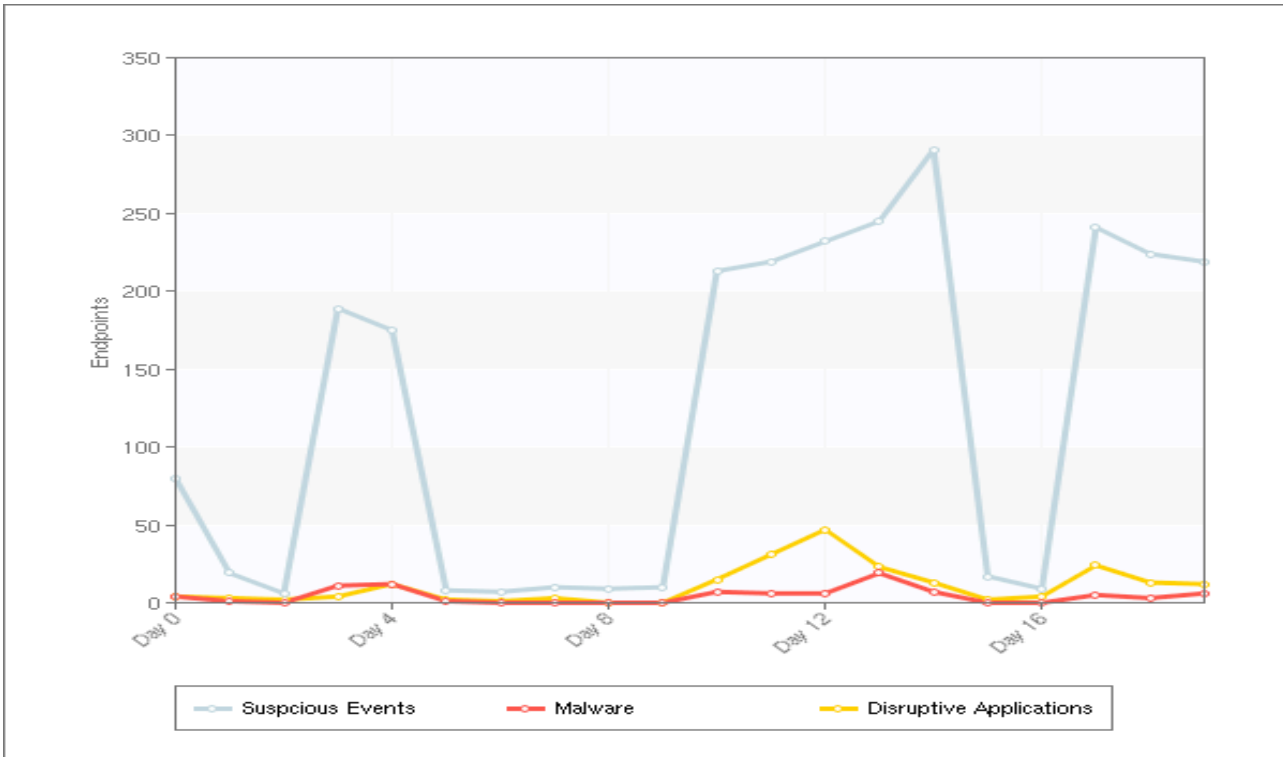
**Malware Infections** - endpoints that are confirmed to be infected with malware

**Suspicious Events** - endpoints that have been detected by TDA to have accessed malicious links, 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

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

## Affected endpoints for past 20 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 |
| Undefined Group*            | 482                  | 0                  | 752                       |
| Department_XXXX             | 24460                | 346                | 0                         |
| <b>TOTAL</b>                | <b>24942</b>         | <b>346</b>         | <b>752</b>                |

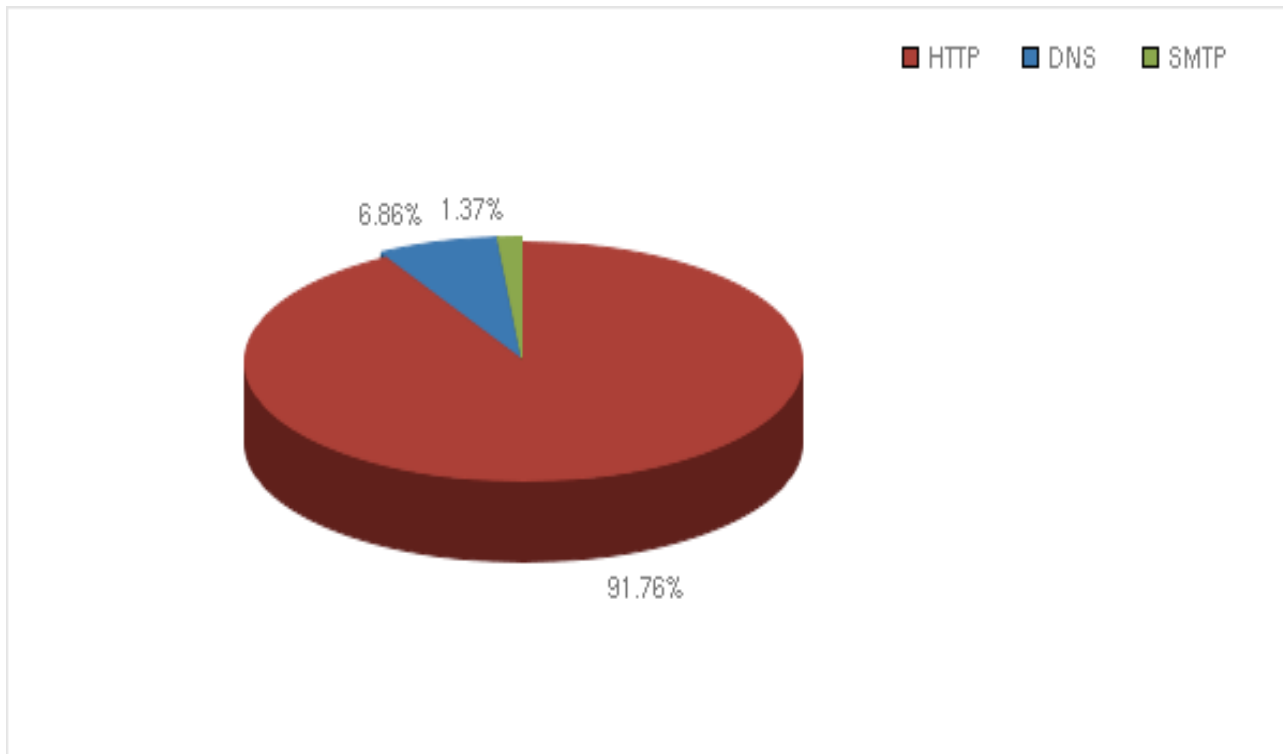
**Malicious URL visits** - total number of malicious URLs visited by endpoints

**Malware Downloaded** - total number of malware files downloaded to end points

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

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

## Threat Protocol Distribution





# Threat Statistics

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

| Threats detected by TMS on endpoints |                 |          |          |                              |
|--------------------------------------|-----------------|----------|----------|------------------------------|
| Group                                | Threat Type     |          |          |                              |
|                                      | Generic malware | IRC bot  | Spam Bot | Information stealing malware |
| Department_XXXX                      | 54              | 3        | 2        | 2                            |
| <b>TOTAL</b>                         | <b>54</b>       | <b>3</b> | <b>2</b> | <b>2</b>                     |

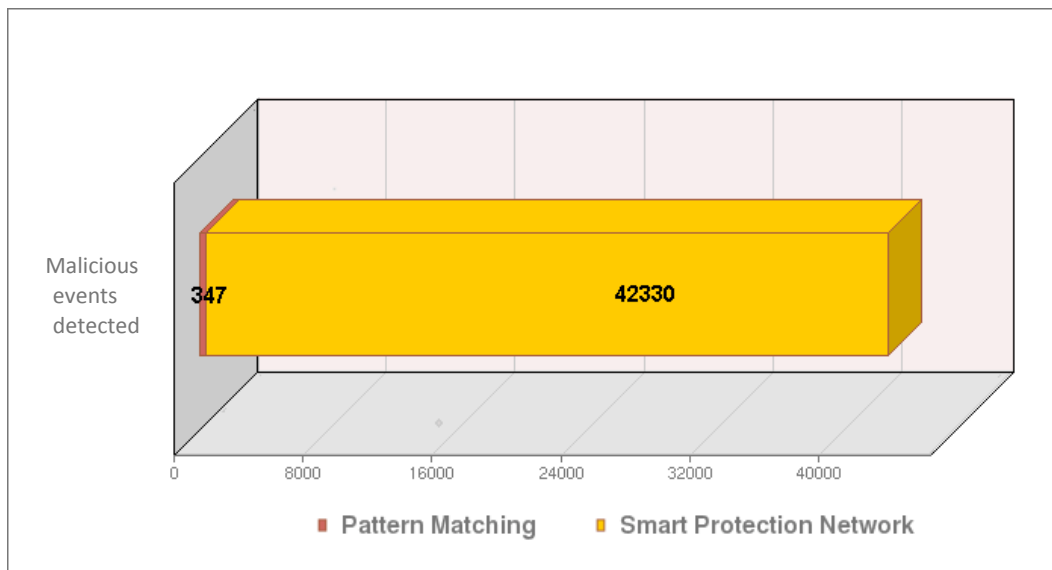
**Generic malware** - Any malicious software that includes Viruses, Worms, Trojans, Password-stealers, Backdoor, etc.

**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).

**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_XXXX                     | 0                 | 99           | 0                 |
| Undefined Group                     | 0                 | 0            | 0                 |
| <b>TOTAL</b>                        | <b>0</b>          | <b>99</b>    | <b>0</b>          |

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

# Document Traffic Statistics

| Outbound Documents |          |      |      |    |         |
|--------------------|----------|------|------|----|---------|
| Filetype           | Protocol |      |      |    |         |
|                    | HTTP     | FTP  | SMTP | IM | Others* |
| Excel              | 1748     | 3    | 14   | 0  | 887     |
| PDF                | 60270    | 1163 | 676  | 0  | 238     |
| Powerpoint         | 1774     | 1    | 0    | 0  | 181     |
| Project            | 0        | 0    | 0    | 0  | 0       |
| Word               | 36758    | 77   | 3    | 0  | 7088    |

\*includes webmail