# Security Checkup

## Threat Analysis Report

Sample Report

COMPUQUIP
CYBERSECURITY

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The following Security Checkup report presents the findings of a security assessment conducted in your network.

The report uncovers where your organization is exposed to security threats, and offers recommendations to address these risks. To assess risk, network traffic was inspected by Compuquip's Check Point engineers to detect a variety of security threats, including: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, and more.

## Malware and Attacks

**287** computers infected with bots

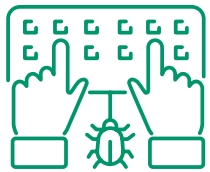
**4.6K** communications with C&C* sites

* C&C - Command and Control. If proxy is deployed, there might be additional infected computers.

**8** known malware downloaded by 10 users

**21** new malware downloaded

New malware variant is a zero-day attack or malicious code with no known anti-virus signature.



**14** unique software vulnerabilities were attempted to be exploited

Indicates potential attacks on computers on your network.

## Data Loss

**114** potential data loss incidents

**6** sensitive data categories

Indicated information sent outside the company or to unauthorized internal users. Information that might be sensitive.

## High Risk Web Access

**18** high risk web applications

**96.2GB**

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

**22** high risk web sites

**409** hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

**15** cloud applications

**12.5GB**

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.

# Key Findings

## Malware and Attacks

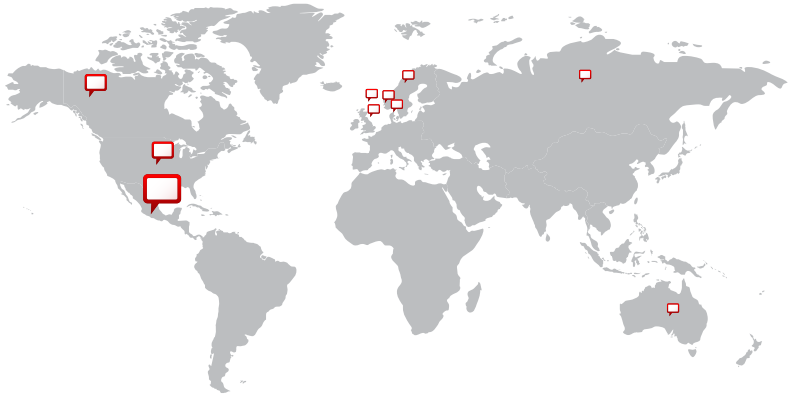
### MACHINES INFECTED WITH BOTS

A bot is malicious software that invades your computer. Bots allow criminals to remotely control your computer to execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DOS) attacks without your knowledge. Bots play a key role in targeted attacks known as Advanced Persistent Threats (APTs). The following table summarizes the bot families and number of infected computers detected in your network.

## Top Bot Families (Top 10 Malware)

| Malware Family* | Infected Computers ** | Communications with Command and Control Center | Destination Country |
|---|---|---|---|
| **Sality** | 61 Computers | 1,453 | Mexico |
| | | | United States |
| | | | Canada |
| **Zeroaccess** | 57 Computers | 684 | China |
| | | | United States |
| | | | United Kingdom |
| | | | Canada |
| | | | Mexico |
| **Zeus** | 54 Computers | 546 | Israel |
| | | | Germany |
| **Pushdo** | 41 Computers | 307 | Russian Federation |
| **Scar** | 32 Computers | 115 | Mexico |
| | | | United States |
| | | | Canada |
| **Virut** | 23 Computers | 97 | Italy |
| | | | Russian Federation |
| **Rustock** | 18 Computers | 66 | Italy |
| | | | France |
| | | | United States |
| | | | Canada |
| **Conficker** | 15 Computers | 50 | Germany |
| | | | Sweden |
| | | | Spain |
| **Koobface** | Computers | 13 | Spain |
| | | | Italy |
| Total: 10 Malware Families | 287 Infected Computers | 4,596 | 13 Countries |

## Command & Control Loactions



* Check Point's malware naming convention: <malware type>.<operating system>.<malware family>.<variant> For more details on specific malware, search the malware name on www.threat-cloud.com ** The total number of infected computers (sources) presents distinct computers.

# Key Findings

## Malware and Attacks

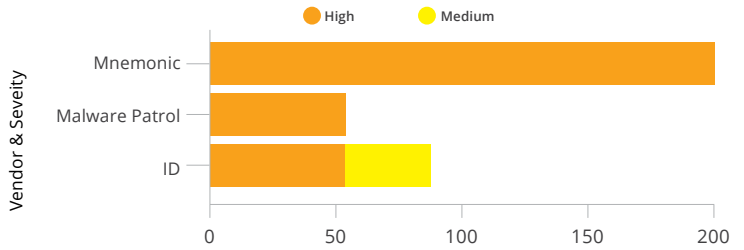
### EXTENDED MALWARE INCIDENTS (CHECK POINT THREATCLOUD INTELLISTORE)

Malware threats were detected by extended security intelligence feeds (via Check Point ThreatCloud IntelliStore*).

## Top Threats by Feed

| Feed | Threat | Severity | | Source | Feed Detection Engine | |
|---|---|---|---|---|---|---|
| **Mnemonic** | Malicious domain.bqzei | | High | 52 Sources | | Anti-Bot |
| | C&C domain.utqzy | | High | 43 Sources | | Anti-Bot |
| | Adware domain.qzf | | High | 20 Sources | | Anti-Bot |
| | Adware domain.qaf | | High | 17 Sources | | Anti-Bot |
| | C&C domain.uteuu | | High | 25 Sources | | Anti-Bot |
| | C&C domain.vaoek | | High | 19 Sources | | Anti-Bot |
| | Malicious domain.bqtmg | | High | 7 Sources | | Anti-Bot |
| | C&C domain.uxqcw | | High | 10 Sources | | Anti-Bot |
| | C&C domain.umzgw | | High | 3 Sources | | Anti-Bot |
| | Adware domain.qbm | | High | 2 Sources | | Anti-Bot |
| | **Total: 10 Threats** | | **High** | **198 Sources** | | **1 Engine** |
| **MalwarePatrol** | URL hosting a malware executable file.dkgoh | | High | 57 Sources | | Anti-Bot |
| | | | | | | Anti-Virus |
| | **Total: 1 Threat** | | **High** | **57 Sources** | | **2 Engine** |
| **ID** | ExploitKit Nuclear.lkfo | | High | 24 Sources | | Anti-Virus |
| | ExploitKit Nuclear.rqdx | | High | 32 Sources | | Anti-Virus |
| | MalwareDownload Generic.bpkp | | Medium | 15 Sources | | Anti-Virus |
| | ExploitKit Angler.bcncr | | Medium | 7 Sources | | Anti-Virus |
| | **Total: 4 Threats** | | **High** | **78 Sources** | **1 Engine** | |
| Total: 3 Feeds | 15 Threats | | High | 333 Sources | 2 Engine | |

## Feeds by Severity




* For more information on Check Point ThreatCloud IntelliStore please refer to http://www.checkpoint.com/products/threatcloud-intellistore/

# Key Findings

## Malware and Attacks

### MACHINES INFECTED WITH ADWARE AND TOOLBARS

Adware and toolbars are potentially unwanted programs designed to display advertisements, redirect search requests to advertising websites, and collect marketing-type data about the user in order to display customized advertising on the computer. Computers infected with these programs should be diagnosed as they may be exposed to follow-up infections of higher-risk malware. The following table summarizes the adware and toolbar malware families and the number of infected computers detected in your network.

**Top Malware Families**

| Adware Name* | Infected Computers** |
|---|---|
| **Adware domain.pzf** | 3 Computers |
| **Adware domain.qaf** | 2 Computers |
| **Adware domain.qbm** | 1 Computer |
| **Adware.Win32.MyWay.A** | 1 Computer |
| **Adware.Win32.Staser.A** | 1 Computer |
| **Adware domain.iqp** | 1 Computer |
| Total: 6 Adware | 570 Computers |

* Check Point's malware naming convention: <malware type>.<operating system>.<malware family>.<variant> For more details on specific malware, search on www.threat-cloud.com

** The total number of infected computers (sources) presents distinct computers

# Key Findings

## Malware and Attacks

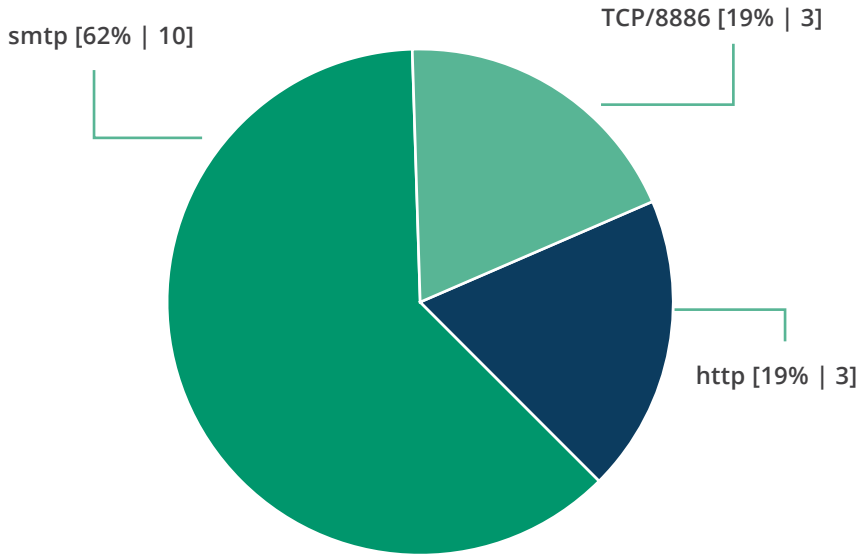
### MALWARE DOWNLOADS (KNOWN MALWARE)

With the increase in sophistication of cyber threats, many targeted attacks begin by exploiting software vulnerabilities in downloaded files and email attachments. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of known malware files detected in your network and the number of the downloading computers. Known malware refers to malware for which signatures exists and therefore should be blocked by an anti-virus system.

### Top Malware Downloads (Top 10 Malware)

| Infected File's Name | Download Computers | Protocol |
|---|---|---|
| **wire.zip** | 3 Computers | smtp |
| **Tranfer.xlsx** | 3 Computers | smtp |
| **tasknow.exe** | 3 Computers | TCP/8886 |
| **Proforma Invoice.Doc** | 2 Computers | smtp |
| **DF4325.Skm** | 2 Computers | http |
| **Invitation.pdf** | 1 Computer | smtp |
| **Your_order.pdf** | 1 Computer | smtp |
| **RH2221.cgi** | 1 Computer | http |
| Total: 8 Infected Files | 10 Computers | 3 Protocols |

### Downloads by Protocol



# Key Findings

## Malware and Attacks

### DOWNLOADS OF NEW MALWARE VARIANTS (UNKNOWN MALWARE)

With cyberthreats becoming increasingly sophisticated, advanced threats often include new malware variants with no existing protections, referred to as "unknown malware." These threats include new (zero-day) exploits, or even variants of known exploits with no existing signatures and therefore are not detectable by standard solutions. Detecting these types of malware requires running them in a virtual sandbox to discover malicious behavior. During the security analysis, a number of malware-related events were detected in your network. The table below summarizes downloads of new malware variants detected in your network.

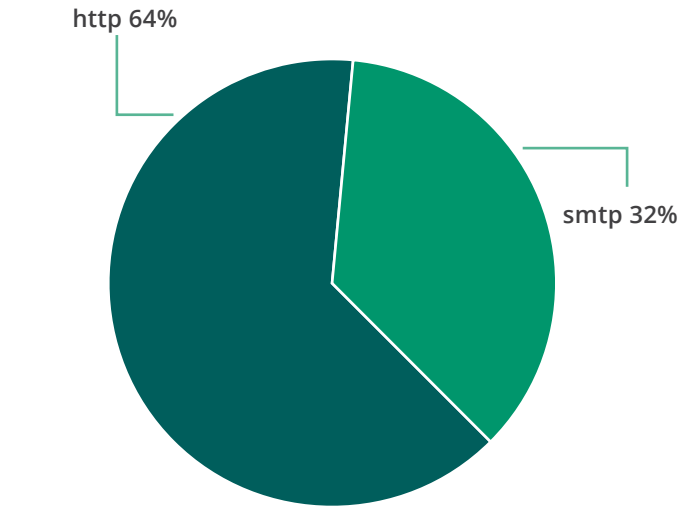
**18.5K**
Total files scanned

**21**
Total malware found

### Downloads of New Malware Variants (Top 5 Malware)

| Infected File Name | Malicious Activity | Downloads | MD5* | Protocols |
|---|---|---|---|---|
| **wire.zip** | Behaves like a known malware (Generic. MALWARE.3d0e )<br>Malware signature matched (Trojan.Win32. Generic.T.kbvx )<br>Unexpected Process Crash | 2 | 09831c2420848703 26865966037ea68f | smtp |
| **0802_41.xls** | Behaves like a known malware (Generic. MALWARE.6c6c )<br>Malicious Filesystem Activity<br>Malicious Registry Activity<br>Unexpected Process Creation | 2 | 289221d50d705238 6379f79358fc547a | http |
| **image0_.png.zip** | A new process was created during the emulation The module creates a suspended process The module executes files or commands The module loads API functions from a DLL dynamically<br>5 more malicious activities | 1 | 6b5dbd65c284c950 fb3fa98c0ac8e924 | smtp |
| **Invoice--0245.zip** | Behaves like a known malware (Generic. MALWARE.84ef ) | 1 | 1efeb7e73eaa0f4dd b8be34e70c36bf6 | http |
| **o.swf** | Malicious Registry Activity Unexpected Process Termination | 1 | 388151bde0f98d7fc 1efb0c3925b6740 | http |
| Total: 21 Infected Files | 16 Activities | 9 Downloads | 8 MD5 | 2 Protocols |

### Downloads by Protocol




* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

# Key Findings

## Malware and Attacks

### ACCESS TO SITES KNOWN TO CONTAIN MALWARE

Organizations can get infected with malware by accessing malicious websites while browsing the Internet, or by clicking on malicious links embedded in received email. The following summarizes events related to sites known to contain malware.

### Top Accessed Sites Known to Contain Malware

| Malicious URL * | Number of Sources | Number of Hits |
|---|---|---|
| 10ensalud.com | 3 | 3 |
| 0i7.ru | 2 | 2 |
| 00xff.net | 1 | 1 |
| 002dh.com | 1 | 1 |
| 17ta.com | 1 | 1 |
| Total: 5 Infected Files | 8 Sources | 8 Hits |

**42 emails**
Received with link to malicious site

* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

# Key Findings

## Malware and Attacks

### ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES

During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes these events.

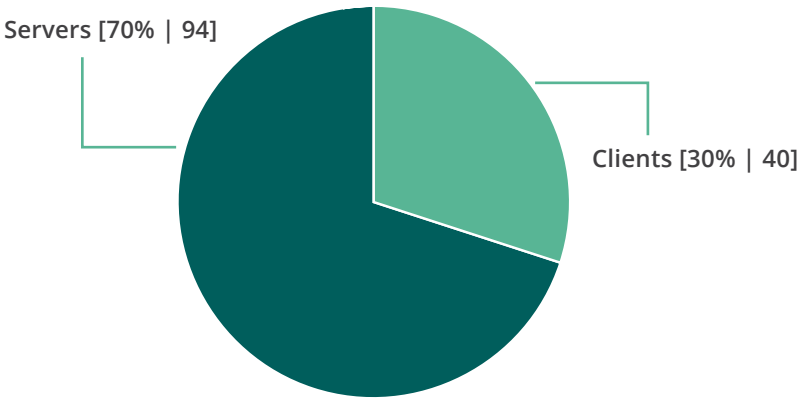
### Attacks on Clients (Top 10 Attacks)

| Attack Name | CVE | Attack Computer | Attackers | Severity | Number of Attacks |
|---|---|---|---|---|---|
| Adobe Flash Player SWF File Buffer Overflow (APSB13-04) | CVE-2009-0520 | 32 | 43 | High | 3,342 |
| Adobe Reader TTF CVT Buffer Overflow (APSB10-09) | CVE-2010-2883 | 31 | 12 | High | 1,232 |
| Internet Explorer ActiveX Navigate Handling Code Execution (MS08-073) | CVE-2008-0078 | 14 | 523 | High | 32 |
| Microsoft Access Snapshot Viewer ActiveX Control Arbitrary File Download | CVE-2008-2463 | 13 | 12 | Medium | 2265 |
| Total: 5 Attacks | | 94 Attacked Computers | 594 Attackers | | 4,884 Attacks |

### Attacks on Servers (Top 10 Attacks)

| Attack Name | CVE | Attack Computer | Attackers | Severity | Number of Attacks |
|---|---|---|---|---|---|
| Microsoft SCCM Reflected Cross-site Scripting (MS12-062) | CVE-2012-2536 | 12 | 56 | Medium | 4,765 |
| Joomla Unauthorized File Upload Remote Code Execution | CVE-2012-2902 | 12 | 33 | Medium | 2,543 |
| Web Servers Malicious HTTP Header Directory Traversal | CVE-2002-0440 | 7 | 123 | High | 126 |
| ImageMagick GIF Comment Processing Off-by-One Buffer Overflow | CVE-2005-0191 | 3 | 4 | Medium | 24 |
| PHP Php-Cgi Query String Parameter Code Execution | CVE-2012-1823 | 2 | 2 | High | 10 |
| Oracle Database Server CREATE_ TABLES SQL Injection | CVE-2009-1991 | 2 | 2 | Low | 5 |
| Total: 5 Attacks | | 40 Attacked Computers | 265 Attackers | | 7,182 Attacks |

### Attacked Targets



# Key Findings

## Malware and Attacks

### DDOS ATTACKS

Denial-of-service (DoS) attacks target networks, systems and individual services flooding them with so much traffic that they either crash or are unable to operate. This effectively denies the service to legitimate users. A DoS attack is launched from a single source to overwhelm and disable the target service. A Distributed  Denial-of-service (DDoS) attack is coordinated and simultaneously launched from multiple sources to overwhelm and disable a target service. During the security analysis, DDoS attacks were detected. The following summarizes the events.

## Summary

**14**
attack types

**70.4K**
total attacks

**13.3MB**
bandwidth utilization

### Top 5 DDoS Attacks

| Attack Name | Severity | Source | Destination | Events |
|---|---|---|---|---|
| Network flood IPv4 UDP | Critical | 59 Sources | 7 attacked<br>4 attacked | 6.4K |
| Network flood IPv4 TCP-SYN | Critical | 2 Sources | 13 attacked<br>21 attacked<br>4 attacked | 5.0K |
| TCP Scan (horizontal) | High | 3 Sources | 2 attacked | 15.55K |
| TCP Scan (vertical) | High | 3 Sources | 13 attacked<br>15 attacked<br>5 attacked | 1.6K |
| TCP Scan | High | 12 Sources | 21 attacked<br>18 attacked<br>17 attacked<br>7 attacked<br>2 attacked | 1.0K |
| Total: 14 Protections | Critical | 118 Sources | 594 Attackers | 70.4 K |

### Top Source Countries

| Attack Name | Attacks |
|---|---|
| Mexico | 41.4K |
| United Kingdom | 5.9K |
| United States | 5.7K |
| Poland | 2.1K |
| France | 1.3K |
| Sweden | 156 |
| China | 24 |
| Serbia | 19 |
| India | 18 |
| Canada | 18 |
| Netherlands | 14 |
| Singapore | 5 |
| Vietnam | 3 |
| Trinidad and Tobago | 2 |
| Kuwait | 2 |
| Total: 16 Countries | 56.6K |

# Key Findings

## High Risk Web Access

### USAGE OF HIGH RISK WEB APPLICATIONS

Web applications are essential to the productivity of every organization, but they also create degrees of vulnerability in its security posture. Remote Administration applications might be legitimate when used by admins and the helpdesk, but please note that some remote access tools can be used for cyber-attacks as well. The following risky web applications were detected in your network, sorted by category, risk level and number of users.

**Top High Risk Web Applications (Top 5 Categories)**

| Application Category | Application Name | Source | Risk Level * | Traffic |
|---|---|---|---|---|
| Proxy Anonymizer | Tor | 7 Sources | 5 Critical | 23 GB |
| | Hola | 4 Sources | 5 Critical | 354 MB |
| | Ultrasurf | 4 Sources | 5 Critical | 239 MB |
| | Hide My Ass | 3 Sources | 5 Critical | 120 MB |
| | OpenVPN | 1 Source | 5 Critical | 32 MB |
| | **Total: 7 Applications** | **16 Sources** | | **26 GB** |
| P2P File Sharing | BitTorrent Protocol | 24 Sources | 4 High | 23 GB |
| | SoulSeek | 22 Sources | 4 High | 22 GB |
| | Xunlei | 19 Sources | 4 High | 12 GB |
| | iMesh | 13 Sources | 4 High | 456 MB |
| | Gnutella Protocol | 8 Sources | 4 High | 56 MB |
| | **Total: 6 Applications** | **73 Sources** | | **61 GB** |
| File Storage & Sharing Applications | Dropbox | 132 Sources | 4 High | 6 GB |
| | Hightail | 54 Sources | 4 High | 3 GB |
| | Mendeley | 9 Sources | 4 High | 123 MB |
| | Zippyshare | 5 Sources | 4 High | 55 MB |
| | Sendspace | 1 Source | 4 High | 3 MB |
| | **Total: 5 Applications** | **201 Sources** | | **9.2 GB** |
| Total: 3 Categories | 18 Applications | 290 Sources | | 96.2 GB |

**96.2 GB**

total high risk web applications traffic

**Top Categories**

| Attack Name | Attacks |
|---|---|
| Proxy Anonymizer | 26 GB |
| P2P File Sharing | 61 GB |
| File Storage & Sharing Applications | 9.2 GB |
| Total: 3 Countries | 96.2 GB |

* RIsk level 5 indicates an application that can bypass security or hide identities. Risk level 4 indicates an application that can cause data leakage or malware infection without user knowledge.

# Key Findings

## High Risk Web Access

### ACCESS TO HIGH RISK WEB SITES

Web use is ubiquitous in business today. But the constantly evolving nature of the web makes it extremely difficult to protect and enforce standards for web usage in a corporate environment. To make matters more complicated, web traffic has evolved to include not only URL traffic, but embedded URLs and applications as well. Identification of risky sites is more critical than ever. Access to the following risky sites was detected in your network, organized by category, number of users, and number of hits.

**Top Risky Websites (Top 5 Categories)**

| Site Category | Site Category | Number of Users | Number of Hits |
|---|---|---|---|
| Phishing | wsq.altervista.org | 7 Users | 59 |
| | applynow.mwexoticspetsforsale.com | 4 Users | 45 |
| | login.marlktplaats.com | 4 Users | 21 |
| | masternard.com | 3 Users | 5 |
| | pro-update.com | 1 User | 3 |
| | **Total: 7 Sites** | **16 Users** | **135** |
| Spam | bgeqwre.com | 24 Users | 65 |
| | bgvlidf.com | 22 Users | 55 |
| | buogbvd.com | 19 Users | 19 |
| | br46cy78son.net | 13 Users | 7 |
| | dq4cmdrzqp.biz | 8 Users | 1 |
| | **Total: 6 Sites** | **73 Users** | **153** |
| Spyware / Malicious Sites | 100footdiet.org | 132 Users | 66 |
| | 0scan.com | 54 Users | 33 |
| | 050h.com | 9 Users | 5 |
| | 123carnival.com | 5 Users | 5 |
| | 0hm.net | 1 User | 3 |
| | **Total: 9 Sites** | **254 Users** | **121** |
| Total: 3 Categories | 22 Sites | 343 Users | 409 |

**Access to sites containing questionable content**

| Site Category | Browse Time (hh:mm:ss) | Traffic Total Bytes |
|---|---|---|
| Illegal / Questionable | 1:16:00 | 15.1MB |
| Sex | 2:42:00 | 8.9MB |
| Gambling | 13:11:00 | 7.4MB |
| Hacking | 00:01:00 | 56.0KB |
| Total: 4 Categories | 17:10:00 | 31.5MB |

Access to non-business websites or to sites containing questionable content can expose an organization to possible productivity loss, compliance and business continuity risks.

# Key Findings

## Data Loss

### DATA LOSS INCIDENTS

Your company's internal data is one of its most valuable assets. Any intentional or unintentional loss can cause damage to your organization. The information below was sent outside the company, or to potentially unauthorized internal users. This information may potentially be sensitive information that should be protected from loss. The following represents the characteristics of the data loss events that were identified during the course of the analysis.

## Summary

**74.3K**
total emails scanned

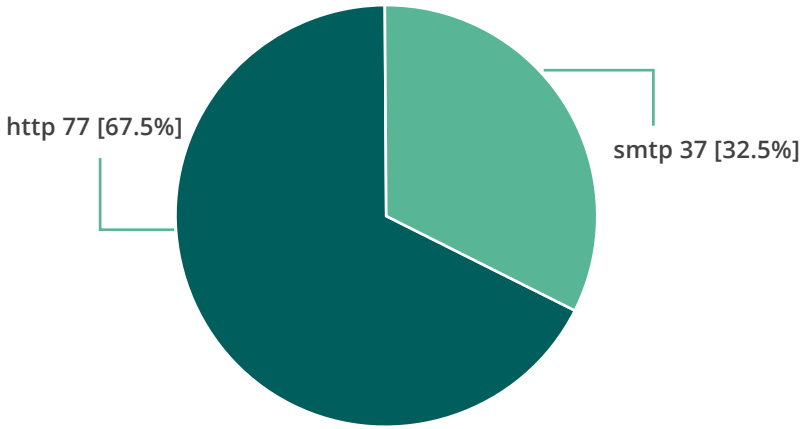
**2**
emails with data loss incidents

**114**
web data loss incidents

### Top Data Types (Top 10 Categories)

| Data Type | Users | Events | Services |
|---|---|---|---|
| Credit Card Numbers | 7 | 54 | http |
| Business Plan | 5 | 32 | smtp |
| Financial Reports | 2 | 12 | http |
| Source Code | 1 | 9 | http |
| Pay Slip File | 3 | 5 | smtp |
| U.S. Social Security Numbers | 1 | 2 | http |
| Total: 6 Data Types | 19 Users | 114 Events | 2 Services |

### Incidents by Protocol



# Key Findings

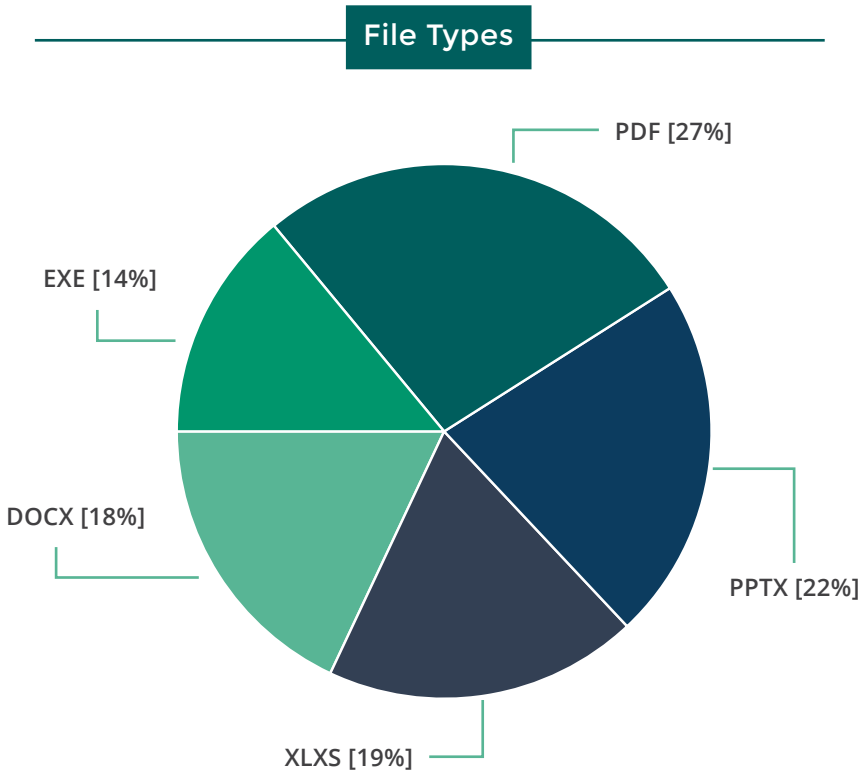
## Data Loss

### FILES UPLOADED TO CLOUD BASED WEB APPLICATIONS

One of the greatest characteristics of Web 2.0 is the ability to generate content and share it with others. This capability comes with significant risk. Sensitive information can get into the wrong hands by storing confidential financial files on cloud-based file storage and sharing services. The following table provides an overview of the types of files uploaded from your organization and the respective file storage and sharing applications used.

**Cloud-Based Web Applications (Top 5 Categories)**

| Site / Application Category | Site / Application | Uploaded Files | Number of Users | File Type |
|---|---|---|---|---|
| File Storage & Sharing Applications | Dropbox | 7 Files | 59 Users | .EXE, .PPTX, .PDF |
| | Hightail | 4 Files | 45 Users | .DOCX, .PPTX |
| | Mendeley | 4 Files | 21 Users | .PDF, .XLXS |
| | Google Drive-web | 4 Files | 13 Users | .EXE, .PDF |
| | Mega | 3 Files | 6 Users | .EXE |
| | **Total: 7 Sites** | **3 Files** | **163 Users** | |
| P2P File Sharing | BitTorrent Protocol | 24 Files | 65 Users | .DOCX, .PPTX |
| | SoulSeek | 22 Files | 55 Users | .PDF, .XLXS |
| | FileMp3.org | 16 Files | 43 Users | .PDF, PPTX |
| | P2P-Radio | 9 Files | 22 Users | .XLXS |
| | Sharebox | 3 Files | 10 Users | .PDF, .XLXS |
| | **Total: 6 Sites** | **76 Files** | **201 Users** | |
| Share Files | Facebook | 132 Files | 66 Users | .DOCX, .PPTX |
| | FreeWire | 42 Files | 23 Users | DOCX. |
| | **Total: 2 Sites** | **174 Files** | **89 Users** | |
| Total: 3 Categories | 15 Sites | 274 Files | 453 Users | |

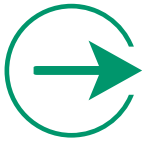


# Key Findings

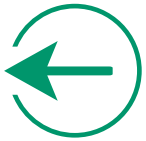
## SCADA Communications

SCADA (Supervisory Control and Data Acquisition) is a type of industrial control system (ICS) that monitors and controls industrial processes. It operates with coded signals over communication channels to provide control of remote equipment. SCADA networks are usually separated from the organizational IT network for security purposes. SCADA protocols detected on the IT network might indicate a security risk with a potential for a security breach. The following SCADA protocols were detected on your network.

## SCADA Communications



**46**
Sources



**23**
Destinations

**9**
Commands

**33**
Ports

### Top SCADA Protocols & Commands (Top 20)

| Protocol & Command | Transactions | Traffic |
|---|---|---|
| BACNet Protocol (Building Automation and Control Networks) | 38 | 4.3GB |
| DNP3 Protocol - freeze and clear | 21 | 123MB |
| EtherNet/IP | 16 | 2.2GB |
| OPC UA - secure conversation message | 2 | 71.0MB |
| DNP3 Protocol - immediate freeze | 2 | 513 MB |
| DNP3 Protocol | 2 | 1.6GB |
| DNP3 Protocol - write | 1 | 1.7GB |
| DNP3 Protocol - ware restart | 1 | 57MB |
| DNP3 Protocol - select | 1 | 321MB |
| Total: 9 Protocols & Commands | 84 Transactions | 10.885GB |

# Key Findings

## Mobile Threats

The following Security Checkup report presents the findings of a security assessment conducted in your network. The report focuses on mobile threats and uncovers where your organization is exposed to them, and offers recommendations to address these risks.

To assess risk, network traffic was inspected by Check Point to detect a variety of security threats, including: mobile malware infections, usage and downloads of high risk mobile apps, download of malicious mobile applications, outdated mobile operating systems, and more.

**547**
Android devices

**433**
iOS devices

**979GB**
total mobile traffic

Mobile devices detected on corporate network (number of devices is based on source IP addresses).

**30**
cloud mobile apps

**19GB** traffic

Examples: Dropbox, Google Drive, OneDrive. Risk of data loss and compliance violations.

**18**
high risk mobile apps

**9GB** traffic

High risk mobile apps are apps that might be used by attackers to monitor and control mobile devices or cause data loss.

**201**
high risk web sites

**855** hits

Examples: Spam, malicious, botnets and phishing web sites. Potential risks: Exposure to web-based threats and network infection.

**20** downloads of malicious apps and malware

**13** infected devices

Download of malicious content such as malicious apps, malware and adware and infected devices communicating with Command and Control servers.

# Key Findings

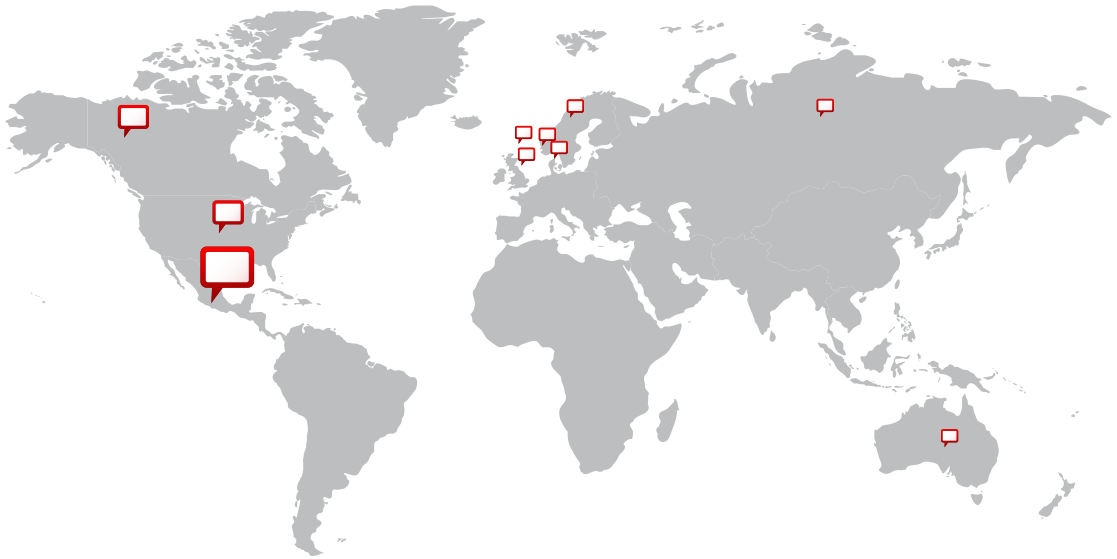
## Mobile Threats

### MOBILE DEVICES INFECTED WITH MALWARE

Mobile malware are malicious software which invade your mobile device. Mobile malware allow criminals to steal sensitive information from a device, take control of its sensors to execute keylogging, steal messages, turn on the video camera, and all this without your knowledge. Mobile malware play a key role in targeted attacks known as Advanced Persistent Threats (APTs). The following table summarizes the mobile malware detected in your network.

| Bot infections (top 20 bots) | | |
|---|---|---|
| **Malware*** | **Infected Devices** | **Communications with Command and Control Center** |
| Plankton | 5 devices | 1,453 |
| Xinyin | 5 devices | 1,265 |
| AndroRAT | 4 devices | 684 |
| BatteryBot | 2 devices | 587 |
| Bosua | 3 devices | 45 |
| HummingBad | 2 devices | 33 |
| SMS-Agent.A | 2 devices | 26 |
| SmsThief | 1 device | 7 |
| SMS-Agent.B | 1 device | 3 |
| Total: 9 malware families | 13 infected devices | 4,103 |

### Command & Control Location



* For more information on specific app, search on http://appwiki.checkpoint.com/

## DOWNLOADS OF MALICIOUS APPS AND MALWARE

With the increased in sophistication in mobile cyber threats, many targeted attacks begin by embedding malware in downloaded apps and files. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of malware by mobile devices.

| Malware downloads (top 20) | | | |
|---|---|---|---|
| **Malware*** | **Downloaded by** | **Downloads** | **MD5** |
| MobileConf.apk | 21 devices | 3 | 582e74467fd100622871fd9cc4dc005c |
| com.android.senscx.apk | 13 devices | 3 | 048b145948a07ab93e24a76dafda8bb7 |
| org.blhelper.vrtwidget.apk | 8 devices | 3 | 76745ce873b151cfd7260e182cbfd404 |
| SystemThread.apk | 7 devices | 3 | b9484ae3403c974db0f721b01bd6c302 |
| com.android.systemUI.apk | 3 devices | 3 | f8645efd5ea2b802d68406207000d59b |
| Pornclub.apk | 2 devices | 2 | 6fa0ffc80d7796748238ad5f1ef3fd71 |
| Settings Tools.apk | 2 devices | 1 | 29dc63afd068dad7a589c680896e5e86 |
| MainActivity.apk | 1 device | 1 | f3867f6159ee25ebf90c8cc0220184ed |
| clean.apk | 1 device | 1 | eeb6777ce814c6c78e7b9bce9f8176e6 |
| Total: 9 malware files | 18 apps | 20 downloads | |

* For more information on specific malware, search on www.threat-cloud.com

# Key Findings

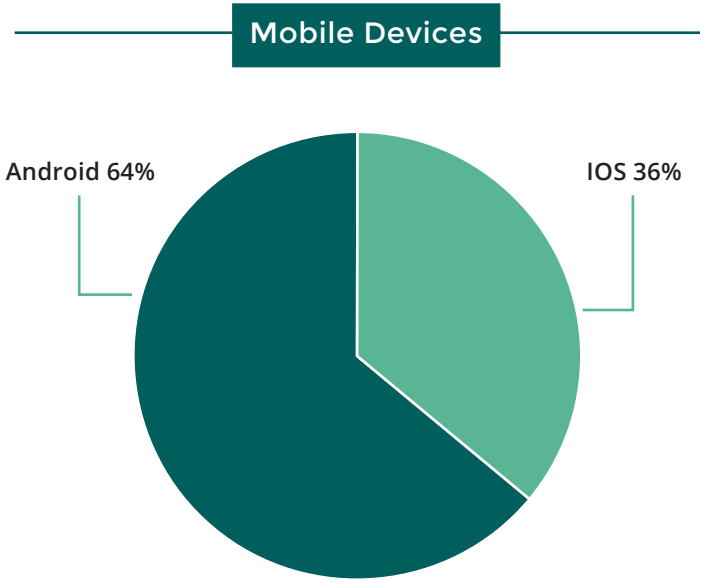
## Mobile Threats

### USAGE OF HIGH RISK MOBILE APPS

Mobile apps are essential to the productivity of every organization, but they also create degrees of vulnerability in its security posture. Remote Administration apps might be legitimate when used by admins and the helpdesk, but when used maliciously, they can allow potential attackers to steal sensitive information from a device, take control of the sensors to execute keylogging, steal messages, turn on video camera, and more. The following risky apps were detected in your network.

**Top high risk mobile apps**

| App Category | App Name* | Risk Level | Devices | Traffic |
|---|---|---|---|---|
| Spyware | Mspy | 4 High | 24 | 5 GB |
| | Spy2Mobile | 4 High | 22 | 2 GB |
| | Bosspy | 4 High | 19 | 1 GB |
| | Mobile Spy | 4 High | 11 | 456 MB |
| | Shadow Copy | 4 High | 5 | 350 MB |
| | My Mobile Watchdog | 4 High | 3 | 120 MB |
| | MobiStealth | 4 High | 2 | 59 MB |
| | TalkLogV | 4 High | 1 | 56 MB |
| Total: 1 category | 18 apps | | 87 | 9GB |




* For more information on specific app, search on http://appwiki.checkpoint.com/

# Key Findings

## Mobile Threats

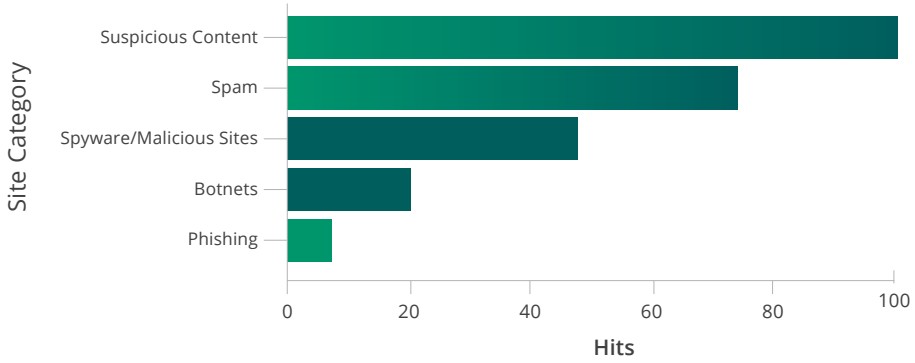
### ACCESS TO HIGH RISK WEB SITES

Web use is ubiquitous in business today. But the dynamic, constantly evolving nature of the web makes it extremely difficult to protect and enforce web usage in a corporate environment. Identification of risky sites is more critical than ever. Access to the following risky sites was detected in your network, organized by category, number of users, then number of hits.

### Top high risk web sites (top 10 sites per category)

| Application/Site | Site | Mobile Users | Hits |
|---|---|---|---|
| Suspicious Content | ad.pxlad.io/ad<br>an.tacoda.net/an/atids.html<br>bam.nr-data.net/1/92a411bc23<br>beacon.securestudies.com/scripts/beaco ...cdn.applight.<br>mobi/applight/2015<br>down.onowcdn.com/testapk<br>dxcnd.cn<br>fbhpadmax.com<br>file1.updrv.com/soft/2012/drivethelife5_s ...19 more Sites | 81 Mobile Users | 104 |
| Spam | a0.awsstatic.net<br>adx.adform.net/adx<br>aptrk.com/g<br>c.ffctdbtr.com<br>cj-cy.com<br>clk.apxadtracking.net/iclk/redirect.php<br>comerciointernacional.com.mx delightfulmotivation.com<br>dl7wen29y4h7i03edf6pm3s6h7nt5oxgpoe.<br>dreamingofgalleries.me<br>16 more Sites | 61 Mobile Users | 73 |

### High risk web sites by category



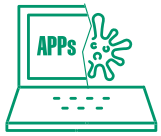

### Access to sites containing questionable content

| Category | Browse Time (hh:mm:ss) | Traffic Total Bytes |
|---|---|---|
| Sex | 21:24:00 | 3.9GB |
| Illegal / Questionable | 3:59:00 | 910.8MB |
| Gambling | 0:10:00 | 11.4MB |
| Hacking | 0:01:00 | 64.0KB |
| T otal: 4 Categories | 25:34 :00 | 4.8GB |

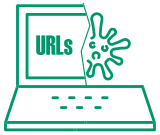
Web Access to non-business websites or to sites containing questionable content can expose an organization to possible productivity loss, compliance and business continuity risks.

# 343 Total Endpoints Detected

## Endpoints Involved in High Risk Web Access and Data Loss Incidents




**23**
running high risk applications




**19**
accessed high risk websites

**22**
users accessed questionable, non-business related websites

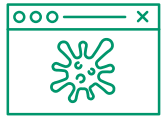
**14**
users involved in potential data loss incidents

## Endpoints Involved in Malware and Attack Incidents

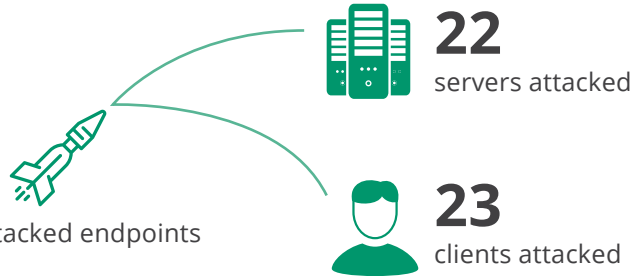
**34**
infected with malware

**44**
downloaded malware

**55**
received email containing link to malicious site



**15**
accessed a site known to contain malware



# Key Findings

## Bandwidth Analysis

### BANDWIDTH UTILIZATION BY APPLICATIONS & WEBSITES

An organization's network bandwidth is usually utilized by a wide range of web applications and sites used by employees. Some are business related and some might not be business related. Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available for important business applications. It is important to understand what is using the network's bandwidth to limit bandwidth consumption of non-business related traffic. The following summarizes the bandwidth usage of your organization sorted by consumed bandwidth.

**Top Applications/Sites (Top 30)**

| Application/Site | Category | Risk Level | Sources | Traffic |
|---|---|---|---|---|
| YouTube | Media Sharing | 2 Low | 151 Sources | 13.6GB |
| Office 365-Outlook | Email | 1 Very Low | 363 Sources | 10.9GB |
| Microsoft SQL Server | Business Application | 2 Low | 189 Sources | 6.4GB |
| Windows Update | Software Update | 1 Very Low | 623 Sources | 4.7GB |
| Server Message Block (SMB) | Network Protocols | 1 Very Low | 491 Sources | 3.7GB |
| Skype | VoIP | 3 Medium | 475 Sources | 2.3GB |
| bestday.com | Travel | -Unknown | 232 Sources | 2.3GB |
| SMTP Protocol | Network Protocols | 3 Medium | 248 Sources | 2.2GB |
| Google Services | Computers / Internet | 2 Low | 437 Sources | 1.9GB |
| Microsoft Dynamics CRM | Business Application | 1 Very Low | 3 Sources | 1.7GB |
| Facebook | Social Network | 2 Low | 226 Sources | 1.6GB |
| oloadcdn.net | Computers / Internet | -Unknown | 3 Sources | 1.5GB |
| Server Message Block (SMB)-write | Network Protocols | 1 Very Low | 33 Sources | 1.2GB |
| Gmail | Email | 3 Medium | 55 Sources | 1.1GB |
| Outlook.com | Email | 3 Medium | 280 Sources | 1.0GB |
| ds.pr.dl.ws.microsoft.com | Computers / Internet | -Unknown | 1 Source | 958.6MB |
| Jabber Protocol (XMPP) | Network Protocol | 2 Low | 391 Sources | 872.6MB |
| Total: 254 Applications/Sites | 34 Categories | 4 Risks | 2,049 Sources | 539.8GB |

**539.8GB**

**Total Traffic Scanned**

### Traffic by Protocol