CHECK POINT™

## SECURITY CHECKUP

# THREAT ANALYSIS REPORT

| Date | Customer | Prepared By |
|---|---|---|
| June 30th, 2022 | Corporate ABC | Check Point Software Technologies |

SECURITY CHECKUP

# THREAT ANALYSIS REPORT

Customer

ABC Corp

Industry

Finance

Company size

500-1000 Employees

Country

USA

Analysis duration

7 Days

Analysis network

Internal Network

Security Gateway version

R81.10

Security device

Check Point Appliances 1800

Traffic inspected by the following Check Point Software Blades:

- ☑ Application Control
- ☑ URL Filtering
- ☑ IPS
- ☑ Anti-bot
- ☑ Anti-virus
- ☑ Threat Emulation

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 Check Point 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

**9** computers infected with bots

**15** communications with C&C* sites

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

**3** known malware downloaded by **3** users

**344** new malware downloaded

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

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

Indicates potential attacks on computers on your network.

## 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.

## SaaS Applications

**15** cloud applications

**12.5GB**

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines

# Table of Contents

# Key Findings

## Cyber Kill Chain

A cyber kill chain reveals the stages of a cyber attack. From early reconnaissance to the goal of data exfiltration.

The kill chain can also be used as a management tool to help continuously improve network defense.

**Pre Infection**

1. Reconnaissance
2. Delivery
3. Exploitation
4. Installation

**Post Infection**

1. Command and Control
2. Propagation

### Pre Infection

**32**
servers were scanned*

**34**
users downloaded malwares

**39**
unique exploits attempts on servers

* Scanned (reconnaissance) Servers – these servers were scanned from the internet for first understanding of open ports and services

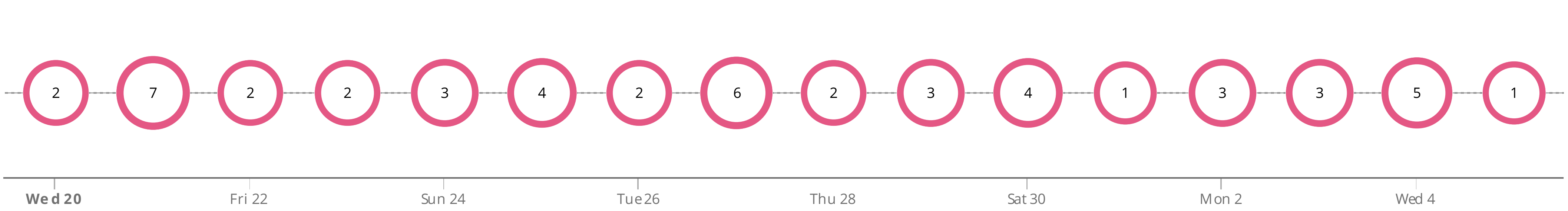
### Post Infection

**15**
malicious connections to C&C servers

**9**
machines are infected

**3**
different malware families were found

### Malicious traffic connected to infected end-point (inbound/outbound connections)



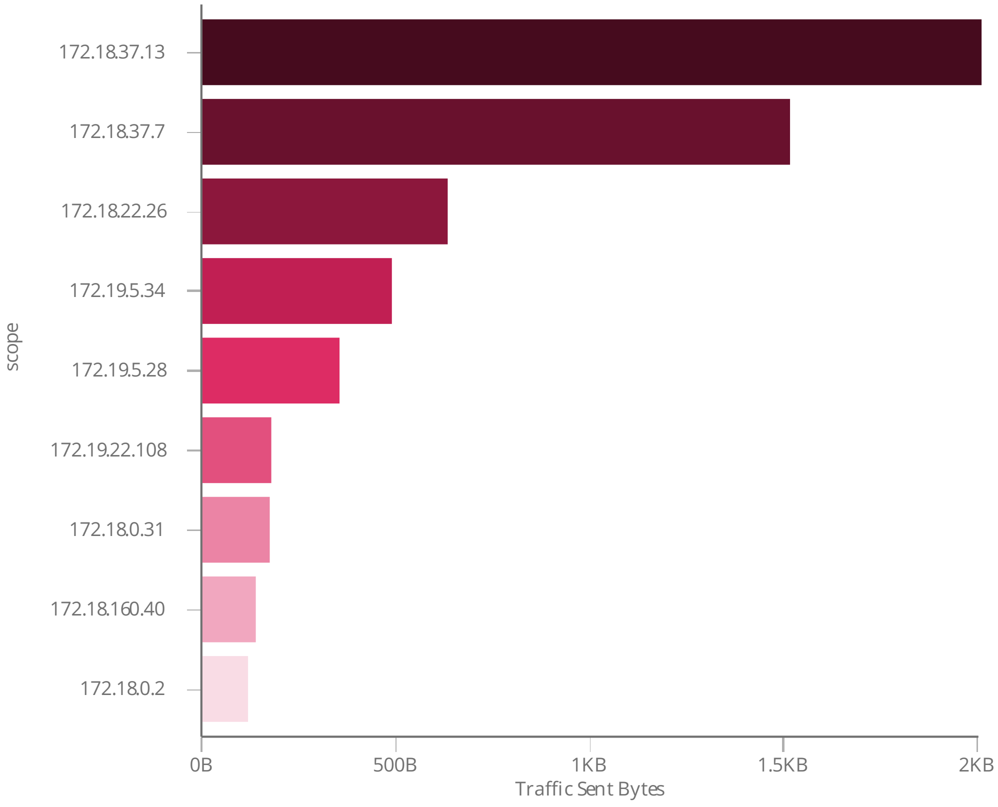
## MACHINES INFECTED WITH MALWARES & BOTS

Bot is a 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 malwares in the network

| Malware Family | Malware Name* | Infected Computers** | Protection Type |
|---|---|---|---|
| | REP.ipohyi | 172.18.0.2<br>172.18.0.31 | DNS Trap |
| Phishing | Phishing.dgodag | 172.19.5.34<br>172.19.22.108 | DNS Trap |
| Joanap | Backdoor.Win32.Joanap.A | 172.18.160.40 | Signature |
| Phishing | Phishing.czuavk | 172.18.37.7 | DNS Trap |
| | REP.hxotqg | 172.18.22.26 | DNS Trap |
| | REP.ioevan | 172.19.5.28 | DNS Trap |
| Roughted | Roughted.jx | 172.18.37.13 | DNS Trap |
| **Total: 3 Families** | **7 Malwares** | **9 Computers** | **2 Protection Types** |

### Top infected machines ***



* 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.

*** Amount of malicious traffic from end-point.

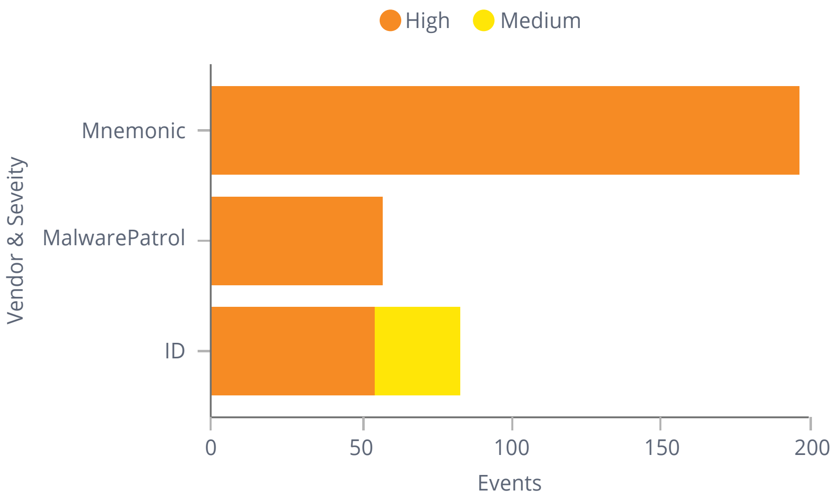
## EXTENDED MALWARE INCIDENTS (CHECK POINT THREATCLOUD INTELLISTORE)

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<br>Anti-Virus |
| | **Total: 1 Threat** | **High** | **57 Sources** | **2 Engines** |
| 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/

## 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.

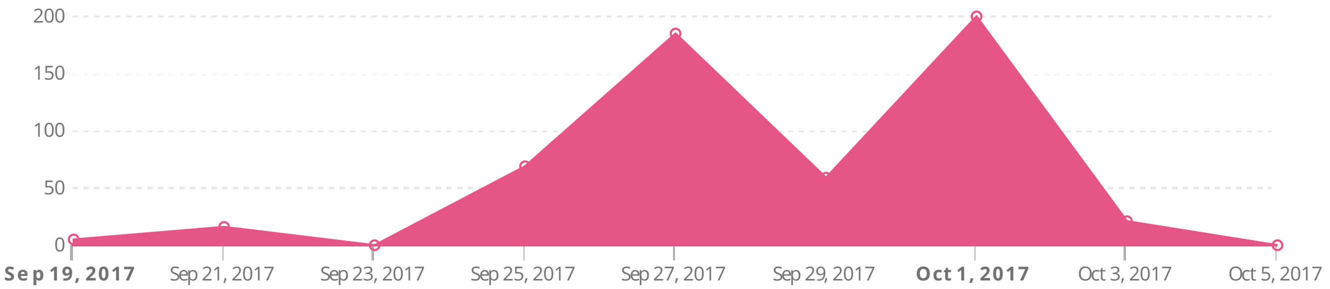
### Top Malware Families

| 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** | **9 Computers** |

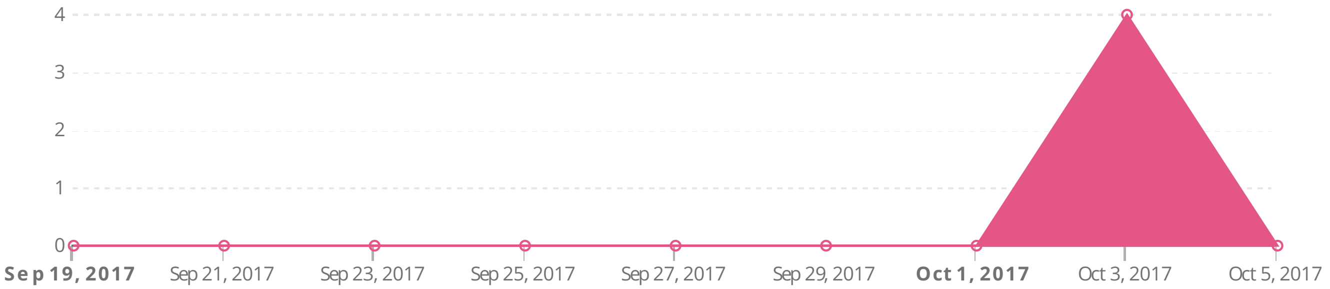
* Check Point's malware naming convention: <malware type>.<operating system>.<malware family>.<variant> For more details on specific malware, search on www.threat-cloud.com

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

## Mail Campaigns - Zero Day Attacks



## Mail Campaigns - Known Malwares



## Malware and Zero Day Incidents

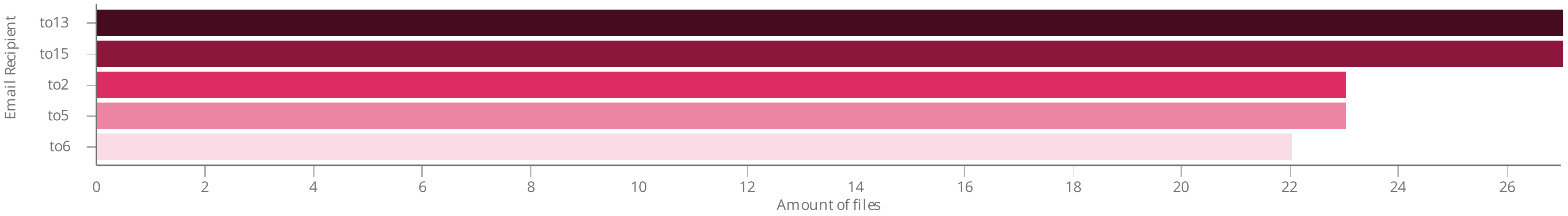
**339** zero day attacks

**3** known malwares

**3** malicious domain reputation activities*

* An email with malicious link was detected

## Top Recipients



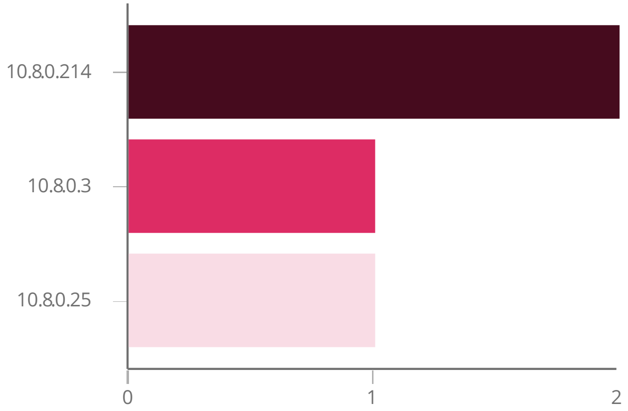
## MALWARE DOWNLOADS (KNOWN MALWARE)

With the increase in sophistication of cyber threats, many targeted attacks begin with 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.

### Malware downloads over http

| Infected File Name | User | Downloaded by | MD5* | Incidents Count |
|---|---|---|---|---|
| noa2.exe | User 1 | 10.8.0.214 | 37945c44a897aa42a66adcab68f560e0 | 2 |
| install_flash_player.exe | User 2 | 10.8.0.25 | fbbdc39af1139aebba4da004475e8839 | 1 |
| **Total: 2 Files** | **2 Users** | **2 Sources** | **2 Files** | **3** |

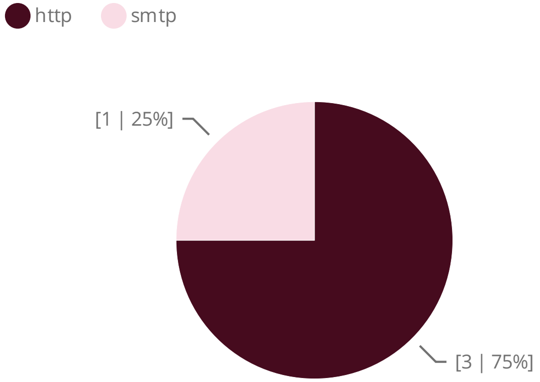
### Top sources downloaded malware



### Malware downloads over smtp

| Infected File Name | User Email | Downloaded by | MD5* | Incident Count |
|---|---|---|---|---|
| QUOTATION 589071_OCT2017 PDF ..ace | to87 | 10.8.0.3 | 31acdfaba00a78d39b7e8369cac90416 | 1 |
| **Total: 1 File** | **1 User** | **1 Source** | **1 File** | **1** |

### Downloads by protocol



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

## DOWNLOADS OF NEW MALWARE VARIANTS (UNKNOWN MALWARE)

With cyber-threats 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.

**1.5K** Total files scanned

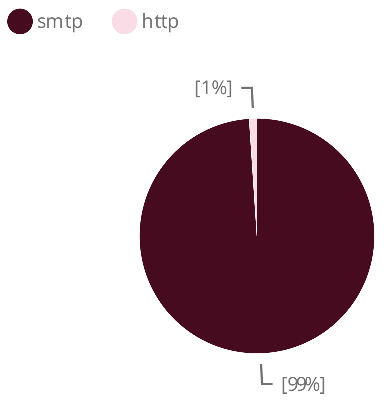
**344** Total malware found
(using sandboxing technology)

### Downloads of new malware variants

| Infected File Name | scope | Malicious Activities | Confidence | Downloads | MD5* | Protocol |
|---|---|---|---|---|---|---|
| New Doc 2017-10-01 - Page 2.7z | 172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.0838 ) | High | 22 | 75fab3cee3f2c0add14f59a1534...<br>3fd8590ca33be86176796f40b9...<br>19 more Files MD5 | smtp |
| New Doc 2017-10-02 - Page 2.7z | 91.243.175.15.<br>122.164.236.1.<br>172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.0531 ) | High | 20 | 09d56ab0cfa15536d14570d5b4..<br>a25bd1667f0022d1ed0693d7d3..<br>15 more Files MD5 | smtp |
| New Doc 2017-10-02 - Page 3.7z | 172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.0dd0 ) | High | 19 | 2781d8fd774372c2f043261ae2a...<br>21f9c24e0d2f79434e2e0c3b412...<br>13 more Files MD5 | smtp |

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

### Malicious downloads by protocol



### Top malicious file types

| File Type | Number of Files | Download |
|---|---|---|
| 7z | 317 Files | 526 |
| zip | 8 Files | 11 |
| rar | 4 Files | 11 |
| jar | 7 Files | 9 |
| pdf | 4 Files | 5 |
| docx | 2 Files | 4 |
| **Total: 8 Types** | **344 Files** | **568 Downloads** |

| Infected File Name | scope | Malicious Activities | Confidence | Downloads | MD5* | Protocol |
|---|---|---|---|---|---|---|
| New Doc 2017-10-02 - Page 1.7z | 172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.235c ) | ▬ High | 16 | 21f9c24e0d2f79434e2e0c3b412f8c82<br>934564cebf2ac8b1bf5188c926909d13<br>9 more Files MD5 | smtp |
| New Doc 2017-10-01 - Page 1.7z | 103.58.144.21<br>172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.6c8c ) | ▬ High | 15 | 55409267c072f07f3c3792665a7c5a01<br>e2595ce25f56a7b0609d1657a5bbb722<br>13 more Files MD5 | smtp |
| New Doc 2017-10-01 - Page 3.7z | 172.17.0.3 | Behaves like a known malware ( Generic.MALWARE.4c0a ) | ▬ High | 9 | aa4b8b2c9b715c5b0eb6ac25ebd989b7<br>acf3e7de88e4795323dae13dde88ec56<br>5 more Files MD5 | smtp |
| attachment20170816-14130-h2sg68.doc | 66.163.186.229<br>74.6.129.214<br>74.6.129.229<br>74.6.133.216<br>74.6.134.216<br>1 more scope | Tampering with normal system operation | ▬ High | 7 | 4F2139E3961202B1DFEAE288AED5CB8F | smtp |
| 58578c7b.exe | 172.18.0.159 | Malicious Registry Activity | ▬ High | 3 | 58578c7b40de85473fa3ed61a8325531 | smtp |
| Invoice-8020082_PDF.zip | 172.17.0.3 | A new process was created during the emulation | ▬ High | 2 | ce8d91a03b1f16fd2650d9266af7769e | smtp |
| MT103_20170929.zip | 84.38.132.131 | Behaves like a known malware ( Generic.MALWARE.cc15 ) | ▬ High | 2 | 90259617abc8e16de350497e2fcb0627 | smtp |
| **Total: 459 Files** | **279 scope** | **362 Malicious activities** | **2 Confidence Levels** | **568** | **344 Files MD5** | **2 Services** |

## ACCESS TO SITES KNOWN TO CONTAIN MALWARE

Organizations can get infected with malware by accessing malicious web sites 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.

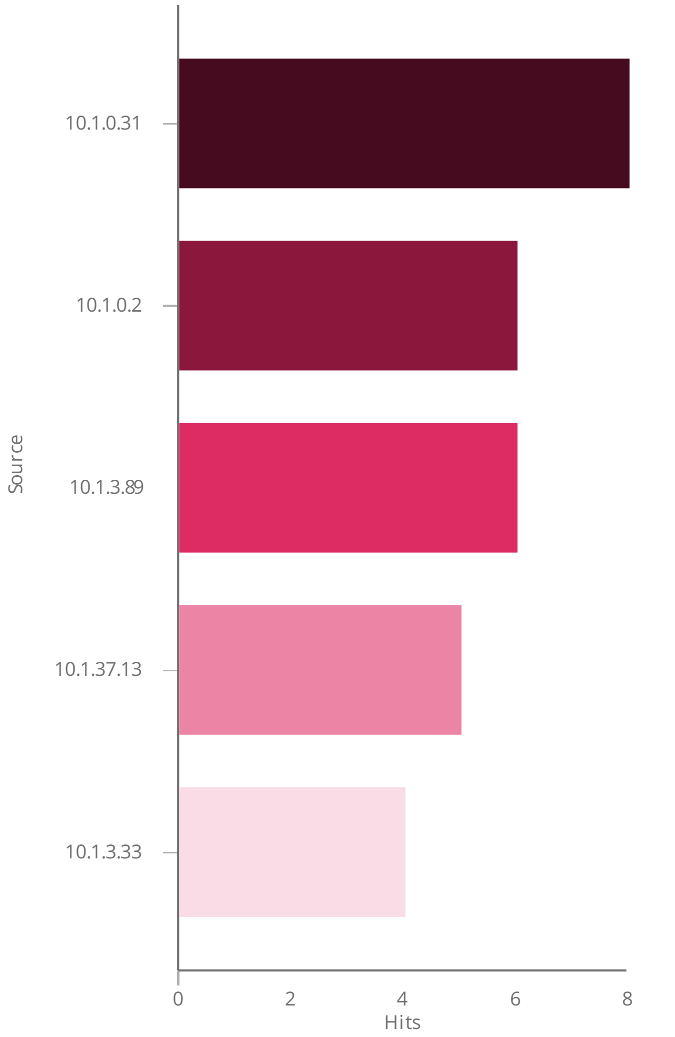
### Top DNS connections to malicious sites

| End-Point IP | Malware Family | Domain | Hits |
|---|---|---|---|
| 172.18.0.31 | Phishing<br>Roughted | clientupdatenw.com<br>gmil.com<br>xml.pdn-1.com | 7 |
| 172.18.0.2 | Phishing<br>Roughted | gmil.com<br>vip.debtcactive.com<br>xml.pdn-1.com | 5 |
| 172.19.0.145 | Phishing | clientupdatenw.com | 4 |
| 172.18.3.89 | Roughted | xml.pdn-1.com | 2 |
| 172.18.37.7 | Phishing | 4iy269pif3b3dd.ru | 1 |
| **Total: 8 scope** | **2 Families** | **5 Domains** | **22** |

### Top HTTP/S connections to malicious sites

| End-Point IP | Malware Family | Domain | Hits |
|---|---|---|---|
| 172.18.2.19<br>172.18.2.20<br>172.18.2.64<br>172.18.3.4<br>172.18.3.50<br>12 more scope | Phishing | http://clientupdatenw.com/?v=3&client=client&os=WIN1...<br>http://boletin.aprendum.com/action.php?id_k=8021&id_...<br>http://clientupdatenw.com/?v=3&client=threshold&os=W...<br>http://clientupdatenw.com/?v=3&client=client&os=WIN6...<br>http://clientupdatenw.com/?v=3&client=trident&os=WIN... | 30 |
| 172.18.3.33<br>172.18.3.89<br>172.18.20.31<br>172.18.20.82<br>172.18.37.13 | Roughted | http://xml.pdn-1.com/redirect?feed=95352&auth=eQ76q...<br>http://xml.pdn-1.com/redirect?feed=72089&auth=PRRXR...<br>http://xml.pdn-1.com/redirect?feed=97557&auth=eQ76q... | 6 |
| **Total: 21 scope** | **2 Families** | **8 Domains** | **36** |

### Top sources accessed malicious sites



* You can analyze suspicious URLs by copying and pasting them into VirusTotal online service at www.virustotal.com

## ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES

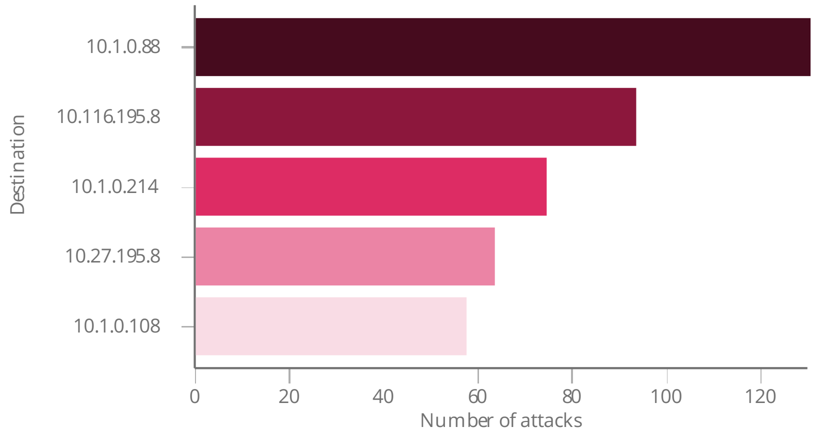
During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes all events with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

### Top attacks and exploited software vulnerabilities

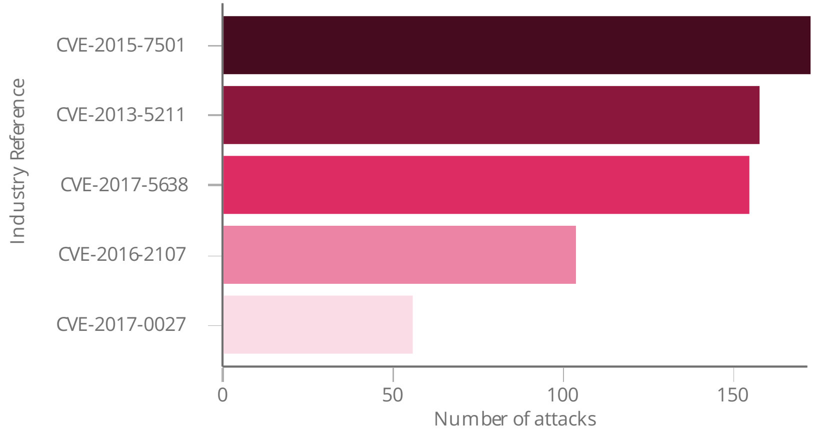
| Attacked Destination | Attack / Exploit | Industry Reference | Attack Source | Events |
|---|---|---|---|---|
| 10.1.0.88 | WebSphere Server and JBoss Platform Apache Commons Collections Remote Code Execution | CVE-2015-7501 | 10.174.140.74 | 24 |
| | | | **Total: 26 Sources** | **82** |
| | Apache Struts2 Content-Type Remote Code Execution | CVE-2017-5638 | 10.112.10.250 | 28 |
| | | | **Total: 3 Sources** | **46** |
| | HP Universal CMDB JMX Console Authentication Bypass | CVE-2014-7883 | 10.156.190.64 | 1 |
| | | | **Total: 1 Source** | **1** |
| | **Total: 4 Attacks / Exploits** | **4 References** | **29 Sources** | **130** |
| 10.116.195.8 | NTP Servers Monlist Command Denial of Service | CVE-2013-5211 | 10.222.94.58 | 22 |
| | | | **Total: 34 Sources** | **93** |
| | **Total: 1 Attack / Exploit** | **1 Reference** | **34 Sources** | **93** |

* You can learn more about the vulnerability that IPS detected by copying and pasting the CVE into Check Point ThreatPortal online service at [https://threatpoint.checkpoint.com/ThreatPortal/](https://threatpoint.checkpoint.com/ThreatPortal/)

### Top targeted end-points



### Top CVEs



| Attacked Destination | Attack / Exploit | Industry Reference | Attack Source | Events |
|---|---|---|---|---|
| 10.1.0.214 | Microsoft Office Information Disclosure (MS17-014: CVE-2017-0027) | CVE-2017-0027 | 10.8.0.214 | 54 |
| | | | **Total: 2 Sources** | **55** |
| | SQL Servers Unauthorized Commands SQL Injection | CVE-2014-3704 | 10.1.22.36 | 10 |
| | | | **Total: 1 Source** | **10** |
| | Microsoft Excel File Format Code Execution (MS12-030) | CVE-2012-0141 | 10.8.0.214 | 9 |
| | | | **Total: 1 Source** | **9** |
| | **Total: 3 Attacks / Exploits** | **3 References** | **3 Sources** | **74** |
| 10.27.195.8 | NTP Servers Monlist Command Denial of Service | CVE-2013-5211 | 10.197.94.58 | 16 |
| | | | **Total: 27 Sources** | **62** |
| | Multiple Vendors NTP Mode 7 Denial of Service | CVE-2009-3563 | 10.118.216.57 | 1 |
| | | | **Total: 1 Source** | **1** |
| | **Total: 2 Attacks / Exploits** | **2 References** | **27 Sources** | **63** |
| 10.1.0.108 | Apache Struts2 Content-Type Remote Code Execution | CVE-2017-5638 | 10.112.10.250 | 32 |
| | | | **Total: 3 Sources** | **50** |
| | WebSphere Server and JBoss Platform Apache Commons Collections Remote Code Execution | CVE-2015-7501 | 10.172.10.250 | 3 |
| | | | **Total: 1 Source** | **3** |
| | HP Universal CMDB JMX Console Authentication Bypass | CVE-2014-7883 | 10.156.190.64 | 2 |
| | | | **Total: 1 Source** | **2** |
| | **Total: 4 Attacks / Exploits** | **4 References** | **4 Sources** | **57** |
| **Total: 111 Destinations** | **28 Attacks / Exploits** | **39 References** | **213 Sources** | **786** |

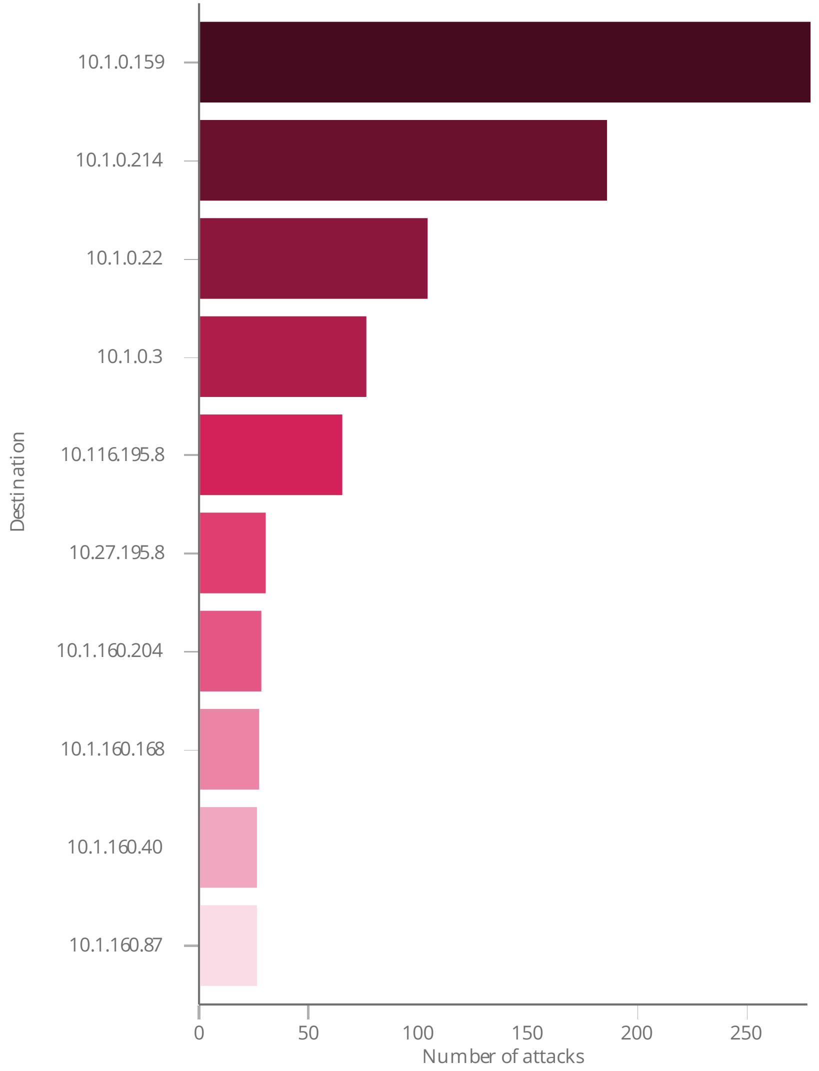
## ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES

The following table summarizes all events that were analyzed and found by Check Point internal ThreatPortal online service.

### Top attacks and exploited vulnerabilities based on internal advisories

| Attack Destination | Attack / Exploit | Attack Source | Events |
|---|---|---|---|
| 10.1.0.159 | Suspicious Executable Mail Attachment | 10.8.0.3 | 154 |
| | Suspicious Mail Attachment Containing JavaScript Code | 10.8.0.3 | 116 |
| | Suspicious Metadata Mail Phishing Containing Archive Attachment | 10.8.0.3 | 4 |
| | **Total: 4 Attacks / Exploits** | **1 Source** | **278** |
| 10.1.0.214 | Sqlmap Automated SQL Injection tool | 10.1.22.36 | 69 |
| | SQL Servers UNION Query-based SQL Injection | 10.1.22.36 | 37 |
| | WordPress HTTP Brute Force Login Attempt | 10.8.0.214 | 19 |
| | **Total: 12 Attacks / Exploits** | **3 Sources** | **185** |
| 10.1.0.22 | Suspicious Metadata Mail Phishing Redirection | 10.2.175.20 | 1 |
| | | 10.3.107.76 | 1 |
| | Suspicious Executable Mail Attachment | 10.116.175.136 | 6 |
| | | 10.2.145.207 | 2 |
| | Suspicious Mail Attachment Containing JavaScript Code | 10.83.38.64 | 2 |
| | | 10.142.186.47 | 2 |
| | **Total: 4 Attacks / Exploits** | **85 Sources** | **103** |
| **Total: 63 Destinations** | **35 Attacks / Exploits** | **199 Sources** | **1.2K** |

### Top targeted end-points



## 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.

### Top scanned servers

| Target end-point | Attack / Exploit | Events | Source |
|---|---|---|---|
| 10.1.85.23 | SIPVicious Security Scanner | 818 | 10.3.178.7<br>10.4.59.54<br>171 more Sources |
| | ZmEu Security Scanner | 17 | 10.91.46.124<br>10.104.45.245<br>4 more Sources |
| | **Total: 7 Attacks / Exploits** | **849** | **192 Sources** |
| 10.1.85.22 | SIPVicious Security Scanner | 821 | 10.3.178.7<br>10.4.59.54<br>170 more Sources |
| | ZmEu Security Scanner | 17 | 10.91.46.124<br>10.104.45.245<br>5 more Sources |
| | **Total: 6 Attacks / Exploits** | **847** | **188 Sources** |
| 10.1.85.21 | SIPVicious Security Scanner | 820 | 10.3.178.7<br>10.4.59.54<br>173 more Sources |
| | ZmEu Security Scanner | 13 | 10.91.46.124<br>10.104.45.245<br>3 more Sources |
| | **Total: 6 Attacks / Exploits** | **844** | **191 Sources** |
| **Total: 32 Destinations** | **11 Attacks / Exploits** | **4.5K** | **247 Sources** |

## 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

| 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

| Application Category | Traffic |
|---|---|
| Proxy Anonymizer | 26 GB |
| P2P File Sharing | 61 GB |
| File Storage & Sharing Applications | 9.2 GB |
| **Total: 3 Categories** | **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.

## 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

| Site Category | Site | 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 |
| Gambing | 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.

## BANDWIDTH UTILIZATION BY APPLICATIONS & WEBSITES

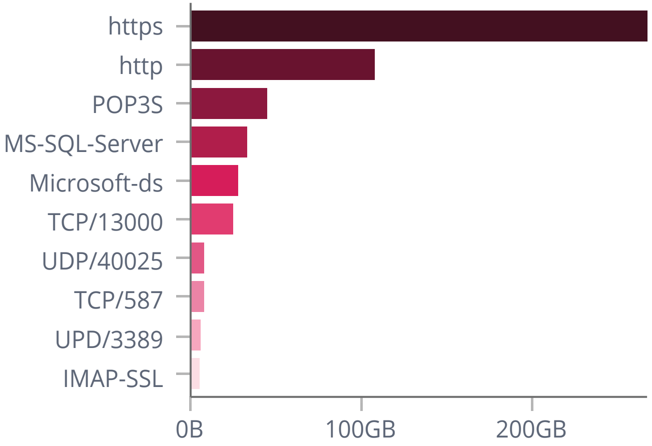
An organization's network bandwidth is usually utilized by a wide range of web applications and sites used by employees. Some are business related and some might not be business related. Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available 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



# CHECK POINT INFINITY

## THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

Growing connectivity along with evolving networks and technologies provide great opportunities for businesses, but also presents new and more sophisticated threats. Securing networks is becoming more complex, often requiring advanced technologies and high level of human expertise. Separate IT environments often drive businesses to apply different point solutions, many of which are focused on detection and mitigation rather than prevention. This reactive approach to cyberattacks is costly and ineffective, complicates security operations and creates inherent gaps in security posture. Enterprises need a more complete architecture that scales with dynamic business demands and focused on prevention to ensure all IT environments are completely protected.

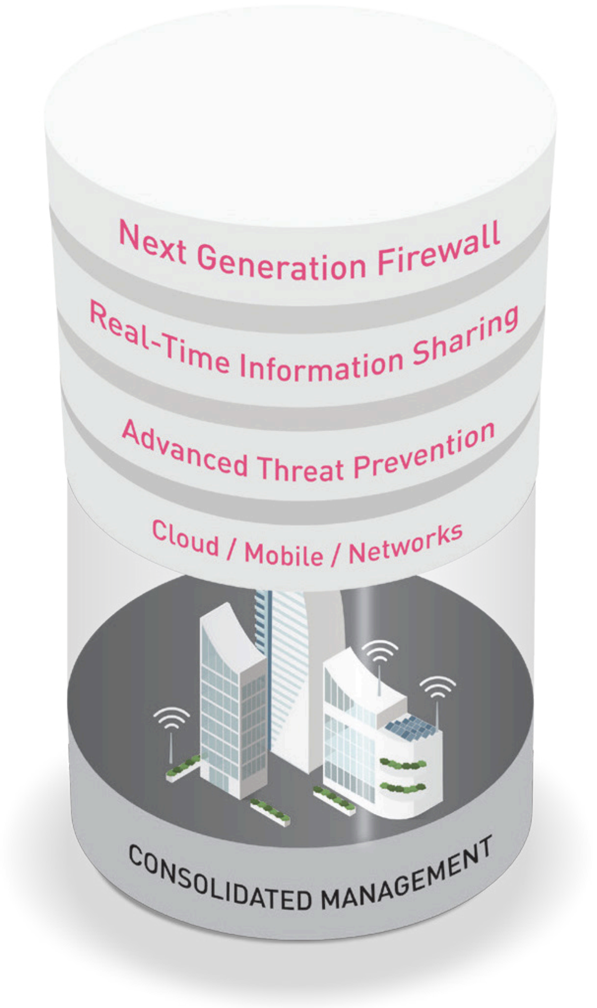
## SOLUTION

Check Point Infinity is the only fully-consolidated cyber security architecture that futureproofs your business and IT infrastructure across all networks, cloud and mobile.
The architecture is designed to resolve the complexities of growing connectivity and inefficient security.

It provides complete threat prevention which seals security gaps, enables automatic, immediate threat intelligence sharing across all security environments, and a unified security management for an utmost efficient security operation.

## UNIFIED SECURITY ACROSS ALL NETWORKS, CLOUD AND MOBILE

Check Point Infinity leverages unified threat intelligence and open interfaces to block attacks on all platforms before they infiltrate the network. The interconnectivity between all Check Point's components delivers consistent security through advanced threat prevention, data protections, web security and more. In addition, the different components share the same set of interfaces and APIs, enabling consistent protection and simplified operation across all networks.
Check Point Infinity also includes the broadest security coverage available for the cloud in today's market, delivering the same levels of advanced security, regardless of the cloud provider selection.
Migration of business applications to mobile has transformed the way we use our devices, exposing us to new types of cyber threats. SandBlast Mobile, the industry's most secure mobile protection, maximizes mobility and security infrastructure with the widest set of integrations in the industry to ensure you stay protected anytime and anywhere.


Next Generation Firewall
Real-Time Information Sharing
Advanced Threat Prevention
Cloud / Mobile / Networks
CONSOLIDATED MANAGEMENT

## PREEMPTIVE CYBER SECURITY

Deploying security which is based on detection and followed by remediation is costly and inefficient, since it allows attackers toinfiltrate the network and cause damage before remediation is done.
Check Point Infinity prevents known and zero-day unknown threats from penetrating the network with SandBlast product family, saving time and the costs associated with remediating the damages.
SandBlast solutions include over 30 different innovative technologies and additional prevention capabilities across all environments:

- Network-based threat prevention for security gateways with best-in-class IPS, AV, post-infection BOT prevention, network Sandboxing (threat emulation) and malware sanitation with Threat Extraction.
- SandBlast Agent endpoint detection and response solution with forensics, anti-ransomware, AV, post-infection BOT prevention and Sandboxing on the endpoint.
- SandBlast Mobile advanced threat prevention for mobile devices protects from threats on the device (OS), in apps, and in the network, and delivers the industry's highest threat catch rate for iOS and Android.
- SandBlast for Office365 cloud, part of Check Point's cloud security offerings.

## CONSOLIDATED SECURITY MANAGEMENT

Managing the entire security network is often complicated and demands high level of human expertise. Check Point Infinity, powered by R80.x security management version, brings all security protections and functions under one umbrella, with a single console which enables easier operation and more efficient management of the entire security network.
The single console introduces unparalleled granular control and consistent security, and provides rich policy management which enables delegation of policies within the enterprise.
The unified management, based on modular policy management and rich integrations with 3rd party solutions through flexible APIs, enables automation of routine tasks to increase operational efficiencies, freeing up security teams to focus on strategic security rather than repetitive tasks.

## SUMMARY

Preventing the next cyber-attack is a possible mission. Check Point has the most advanced technologies and threat prevention solutions for the entire IT infrastructure.
Check Point Infinity architecture unifies the entire IT security, providing real-time shared threat intelligence and a preemptive protection – all managed by a single, consolidated console.

Future-proof your business and ensure business continuity with the architecture that keeps you protected against any threat, anytime and anywhere.

## BENEFITS

- Prevention-driven cyber security, powered by the most advanced threat prevention solutions against known and unknown threats.
- Consistent security across all Check Point components with shared threat intelligence across networks, cloud and mobile.
- Unified and efficient management of the entire security network through a single pane of glass.
- Rich integrations with 3rd party solutions with flexible APIs.

## About Check Point

Check Point Software Technologies' mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

**www.checkpoint.com**

## CORPORATE HEADQUARTERS

**United States**
Check Point Software Technologies Inc.
959 Skyway Road Suite 300
San Carlos, CA 94070
1-800-429-4391

**International**
Check Point Software Technologies Ltd.
5 Ha'Solelim Street
Tel Aviv 67897, Israel
+972-3-753-4555

Please contact us for more information and to schedule your onsite assessment:

Within the US: 866-488-6691

Outside the US: +44 2036087492

CHECK POINT™

# SECURITY CHECKUP

THREAT ANALYSIS REPORT