

SECURITY CHECKUP

THREAT ANALYSIS REPORT

Date
Jan 6th 2020

Customer
ABC Corp

Prepared by:
Check Point Software Technologies

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
R80

Security device
Check Point Appliances 4800

Traffic inspected by the following Check Point Software Blades:

- ☒ Application Control
- ☒ URL Filtering
- ☒ IPS
- ☒ Anti-bot
- ☒ Anti-virus
- ☒ Threat Emulation
- ☒ Threat Extraction
- ☒ Content Awareness

Table of Contents



EXECUTIVE SUMMARY



KEY FINDINGS



MALWARE & ATTACKS



HIGH RISK WEB ACCESS



DATA LOSS



MOBILE THREATS



ENDPOINTS



BANDWIDTH ANALYSIS



CHECK POINT INFINITY

▶ CHECK POINT INFINITY

▶ ABOUT CHECK POINT

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.

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

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*



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

34

users downloaded malwares



39

unique exploits attempts on servers



Post Infection

15

malicious connections to C&C servers



9

machines are infected

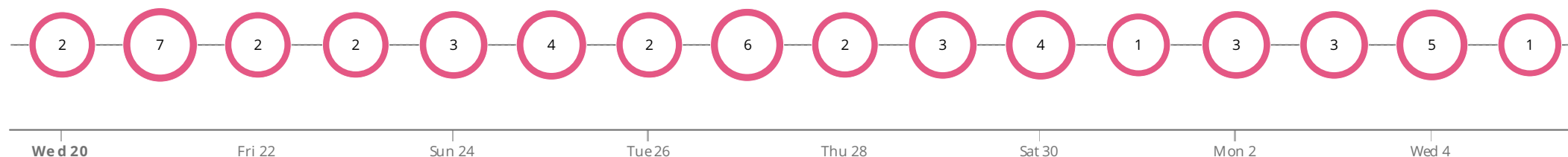


3

different malware families were found



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



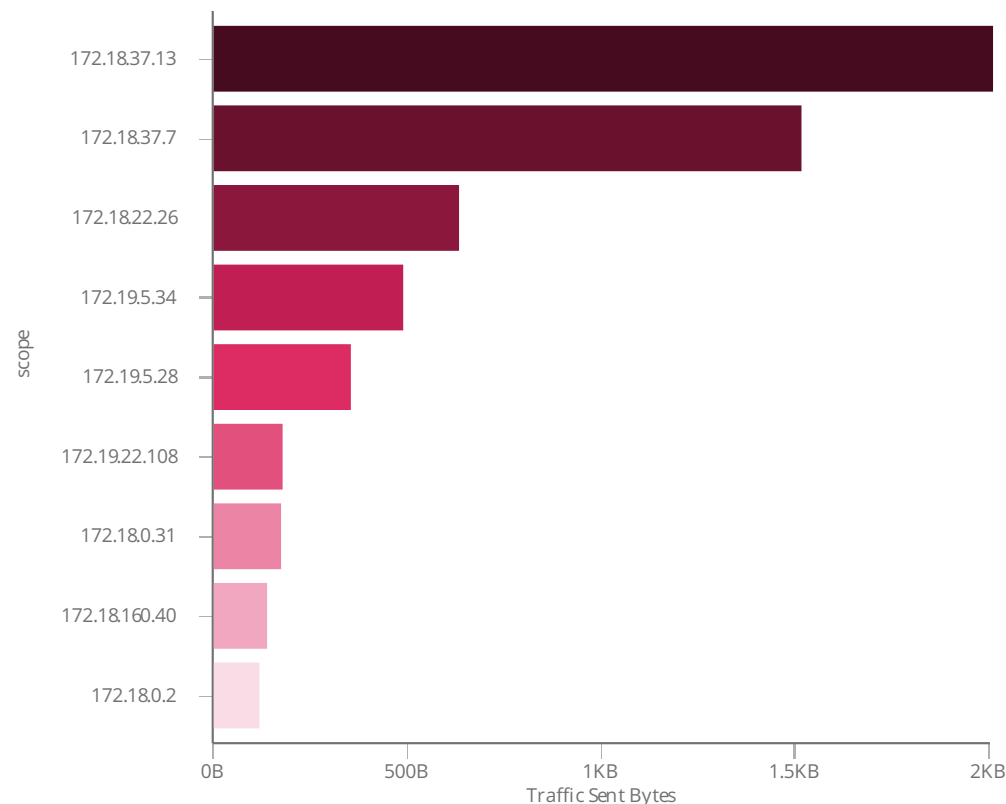
MACHINES INFECTED WITH MALWARES & BOTS

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	172.18.0.2 172.18.0.31	🗨️ DNS Trap
Phishing	Phishing.dgodag	172.19.5.34 172.19.22.108	🗨️ 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.

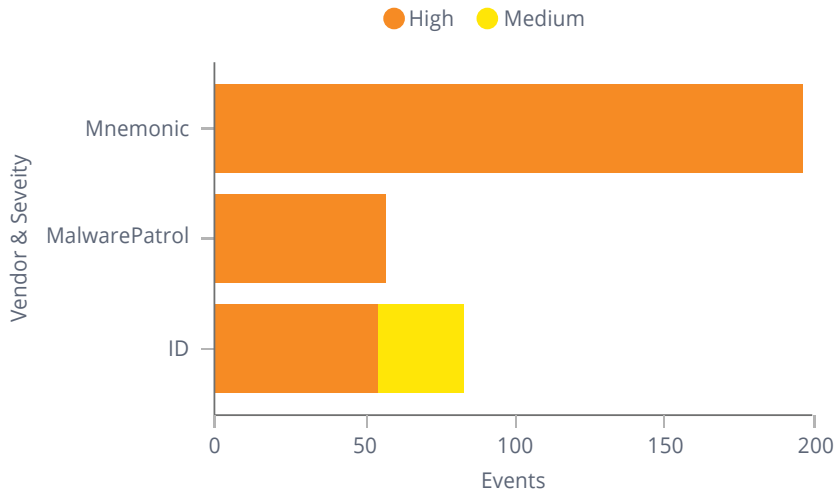
EXTENDED MALWARE INCIDENTS (CHECK POINT THREATCLOUD INTELLISTORE)

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

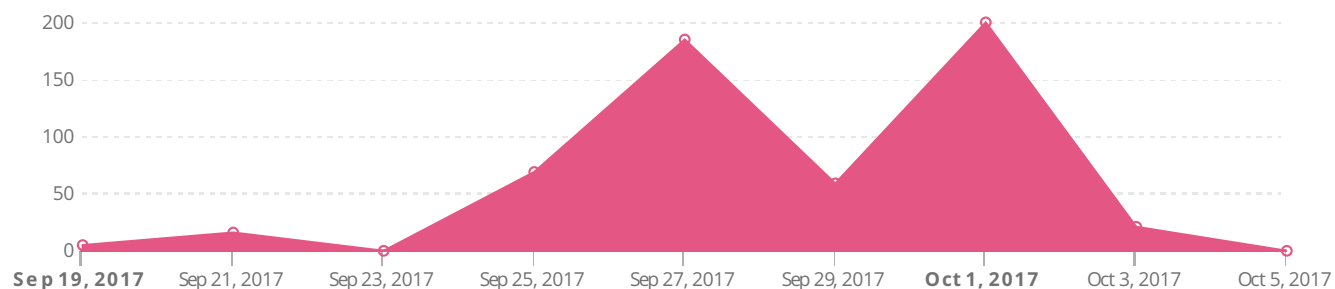
Adware Name*	Infected Computers**
Adware domain.pzf	3 Computers
Adware domain.qaf	2 Computers
Adware domain.qbm	1 Computer
Adware.Win32.MyWay.A	1 Computer
Adware.Win32.Staser.A	1 Computer
Adware domain.iqp	1 Computer
Total: 6 Adware	9 Computers

* 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

KEY FINDINGS ▶ MALICIOUS MAIL CAMPAIGN

Mail Campaigns - Zero Day Attacks



Mail Campaigns - Known Malwares



Malware and Zero Day Incidents

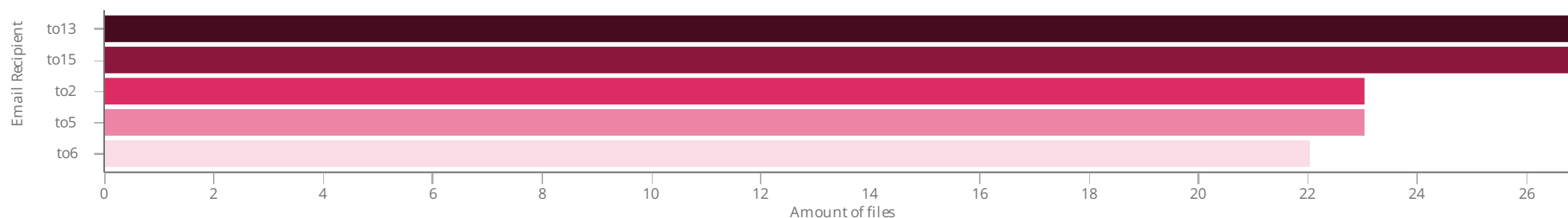
339 zero day attacks

3 known malwares

3 malicious domain reputation activities*

* An email with malicious link was detected



Top Recipients



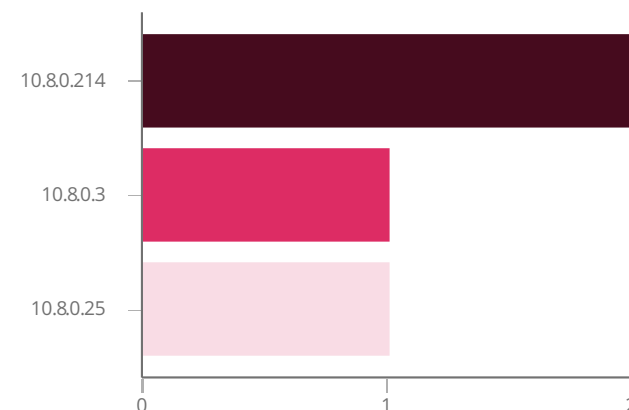
MALWARE DOWNLOADS (KNOWN MALWARE)

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

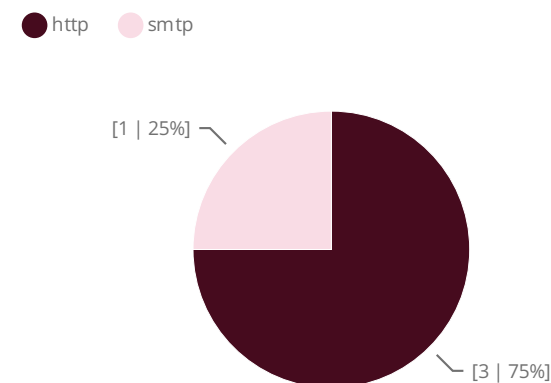
Top sources downloaded malware



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.

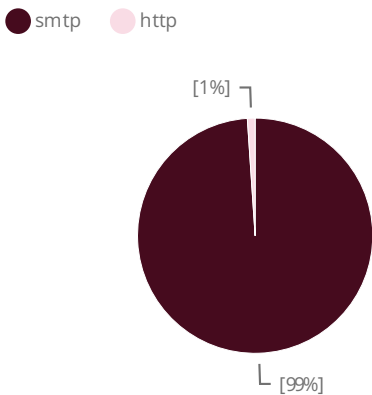
1.5K Total files scanned

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... 3fd8590ca33be86176796f40b9... 19 more Files MD5	smtp
New Doc 2017-10-02 - Page 2.7z	91.243.175.15. 122.164.236.1. 172.17.0.3	Behaves like a known malware (Generic.MALWARE.0531)	High	20	09d56ab0cfa15536d14570d5b4.. a25bd1667f0022d1ed0693d7d3.. 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... 21f9c24e0d2f79434e2e0c3b412... 13 more Files MD5	smtp

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

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

KEY FINDINGS ▶ MALWARE AND ATTACKS

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 934564cebf2ac8b1bf5188c926909d13 9 more Files MD5	smtp
New Doc 2017-10-01 - Page 1.7z	103.58.144.21 172.17.0.3	Behaves like a known malware (Generic.MALWARE.6c8c)	 High	15	55409267c072f07f3c3792665a7c5a01 e2595ce25f56a7b0609d1657a5bbb722 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 acf3e7de88e4795323dae13dde88ec56 5 more Files MD5	smtp
attachment20170816-14130-h2sg68.doc	66.163.186.229 74.6.129.214 74.6.129.229 74.6.133.216 74.6.134.216 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.

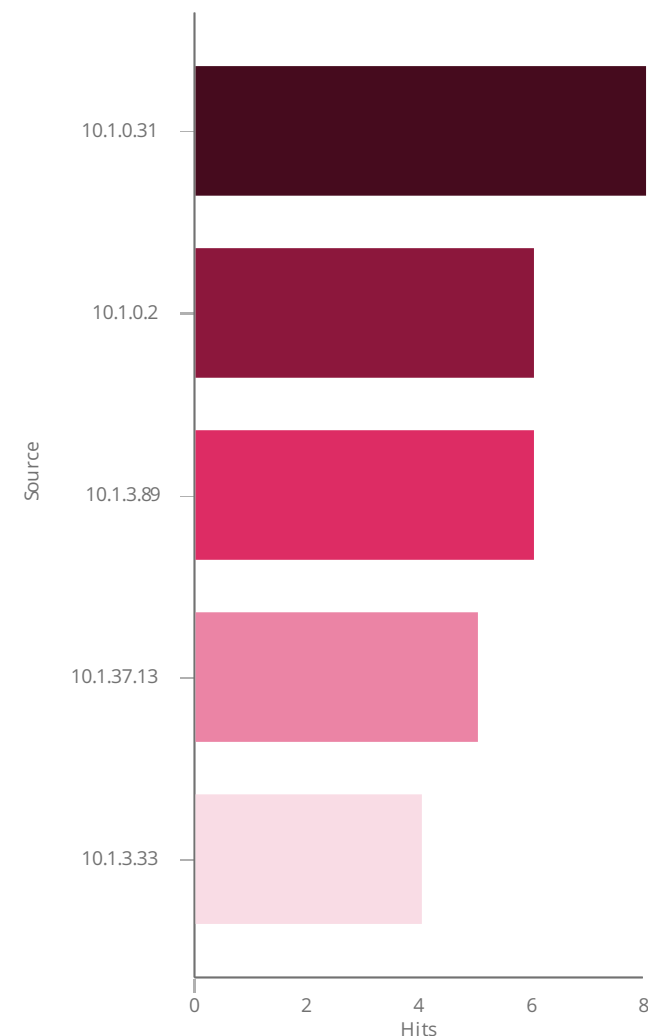
Top DNS connections to malicious sites

End-Point IP	Malware Family	Domain	Hits
172.18.0.31	Phishing Roughted	clientupdatenw.com gmil.com xml.pdn-1.com	7
172.18.0.2	Phishing Roughted	gmil.com vip.debtactive.com 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
172.18.2.19 172.18.2.20 172.18.2.64 172.18.3.4 172.18.3.50 12 more scope	Phishing	http://clientupdatenw.com/?v=3&client=client&os=WIN1... http://boletin.aprendum.com/action.php?id_k=8021&id_... http://clientupdatenw.com/?v=3&client=threshold&os=W... http://clientupdatenw.com/?v=3&client=client&os=WIN6... http://clientupdatenw.com/?v=3&client=trident&os=WIN...	30
172.18.3.33 172.18.3.89 172.18.20.31 172.18.20.82 172.18.37.13	Roughted	http://xml.pdn-1.com/redirect?feed=95352&auth=eQ76q... http://xml.pdn-1.com/redirect?feed=72089&auth=PRRXR... 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

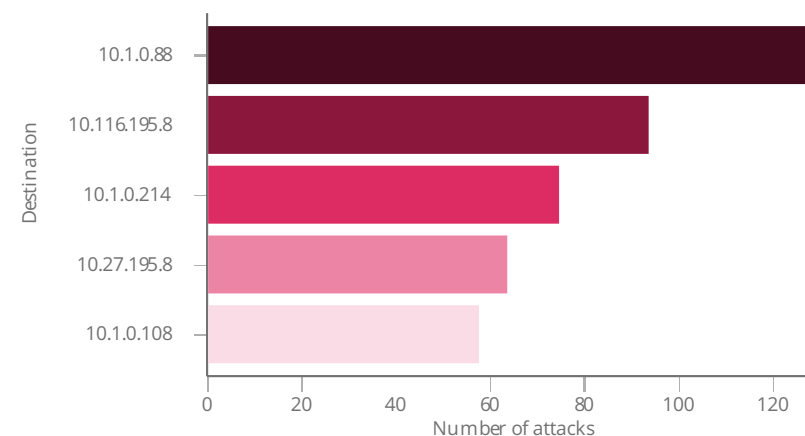
During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes all events with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

Top attacks and exploited software vulnerabilities

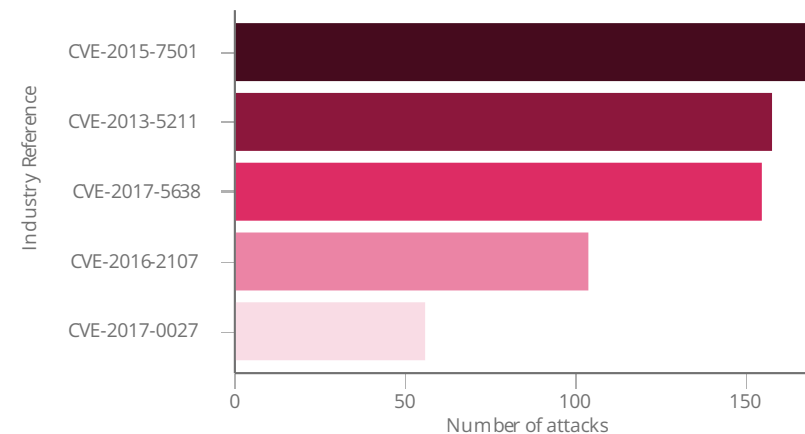
Attacked Destination	Attack / Exploit	Industry Reference	Attack Source	Events
10.1.0.88	WebSphere Server and JBoss Platform Apache Commons Collections Remote Code Execution	CVE-2015-7501	10.174.140.74	24
			Total: 26 Sources	82
	Apache Struts2 Content-Type Remote Code Execution	CVE-2017-5638	10.112.10.250	28
			Total: 3 Sources	46
10.116.195.8	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/>












Top targeted end-points



Top CVEs



KEY FINDINGS ▸ MALWARE AND ATTACKS

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

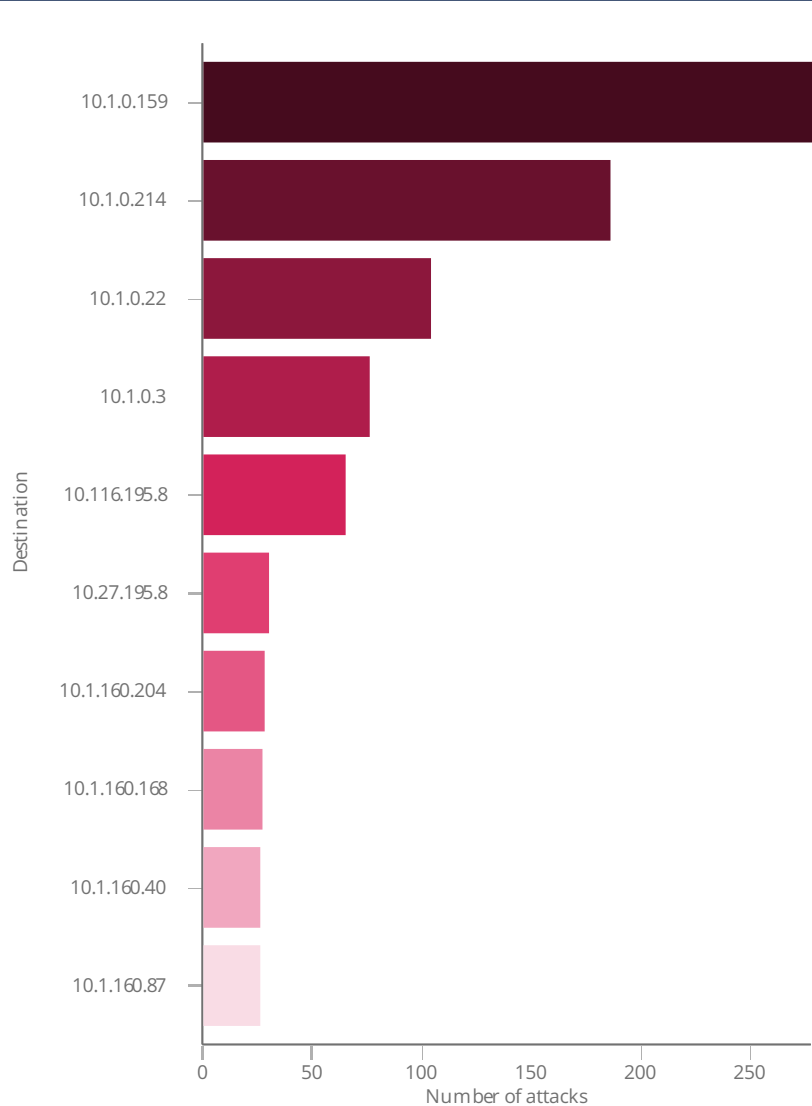
ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES

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		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		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		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  10.4.59.54 171 more Sources
	ZmEu Security Scanner	17	 10.91.46.124  10.104.45.245 4 more Sources
	Total: 7 Attacks / Exploits	849	192 Sources
 10.1.85.22	SIPVicious Security Scanner	821	 10.3.178.7  10.4.59.54 170 more Sources
	ZmEu Security Scanner	17	 10.91.46.124  10.104.45.245 5 more Sources
	Total: 6 Attacks / Exploits	847	188 Sources
 10.1.85.21	SIPVicious Security Scanner	820	 10.3.178.7  10.4.59.54 173 more Sources
	ZmEu Security Scanner	13	 10.91.46.124  10.104.45.245 3 more Sources
	Total: 6 Attacks / Exploits	844	191 Sources
Total: 32 Destinations	11 Attacks / Exploits	4.5K	247 Sources

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 DDoS Attacks

Attack Name	Severity	Source	Destination	Events
Network flood IPv4 UDP	<div><div></div><div></div><div></div><div></div></div> Critical	59 Sources	<div><div></div> 7 attacked</div> <div><div></div> 4 attacked</div>	6.4K
Network flood IPv4 TCP-SYN	<div><div></div><div></div><div></div><div></div></div> Critical	2 Sources	<div><div></div> 13 attacked</div> <div><div></div> 21 attacked</div> <div><div></div> 4 attacked</div>	5.0K
TCP Scan (horizontal)	<div><div></div><div></div><div></div><div></div></div> High	3 Sources	<div><div></div> 2 attacked</div>	15.55K
TCP Scan (vertical)	<div><div></div><div></div><div></div><div></div></div> High	3 Sources	<div><div></div> 13 attacked</div> <div><div></div> 15 attacked</div> <div><div></div> 5 attacked</div>	1.6K
TCP Scan	<div><div></div><div></div><div></div><div></div></div> High	12 Sources	<div><div></div> 21 attacked</div> <div><div></div> 18 attacked</div> <div><div></div> 17 attacked</div> <div><div></div> 7 attacked</div> <div><div></div> 2 attacked</div>	1.0K
Total: 14 Protections	<div><div></div><div></div><div></div><div></div></div> Critical	118 Sources	64 Destinations	70.4 K































Top Source Countries

Source Country	Attacks
<div><div></div> Mexico</div>	41.4K
<div><div></div> United Kingdom</div>	5.9K
<div><div></div> United States</div>	5.7K
<div><div></div> Poland</div>	2.1K
<div><div></div> France</div>	1.3K
<div><div></div> Sweden</div>	156
<div><div></div> China</div>	24
<div><div></div> Serbia</div>	19
<div><div></div> India</div>	18
<div><div></div> Canada</div>	18
<div><div></div> Netherlands</div>	14
<div><div></div> Singapore</div>	5
<div><div></div> Vietnam</div>	3
<div><div></div> Trinidad and Tobago</div>	2
<div><div></div> Kuwait</div>	2
Total: 16 Countries	56.6K

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	 Critical	23 GB
	 Hola	4 Sources	 Critical	354 MB
	 Ultrasurf	4 Sources	 Critical	239 MB
	 Hide My Ass	3 Sources	 Critical	120 MB
	 OpenVPN	1 Source	 Critical	32 MB
	Total: 7 Applications	16 Sources		26 GB
P2P File Sharing	 BitTorrent Protocol	24 Sources	 High	23 GB
	 SoulSeek	22 Sources	 High	22 GB
	 Xunlei	19 Sources	 High	12 GB
	 iMesh	13 Sources	 High	456 MB
	 Gnutella Protocol	8 Sources	 High	56 MB
	Total: 6 Applications	73 Sources		61 GB
File Storage & Sharing Applications	 Dropbox	132 Sources	 High	6 GB
	 Hightail	54 Sources	 High	3 GB
	 Mendeley	9 Sources	 High	123 MB
	 Zippyshare	5 Sources	 High	55 MB
	 Sendspace	1 Source	 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.marlktpplaats.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.

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

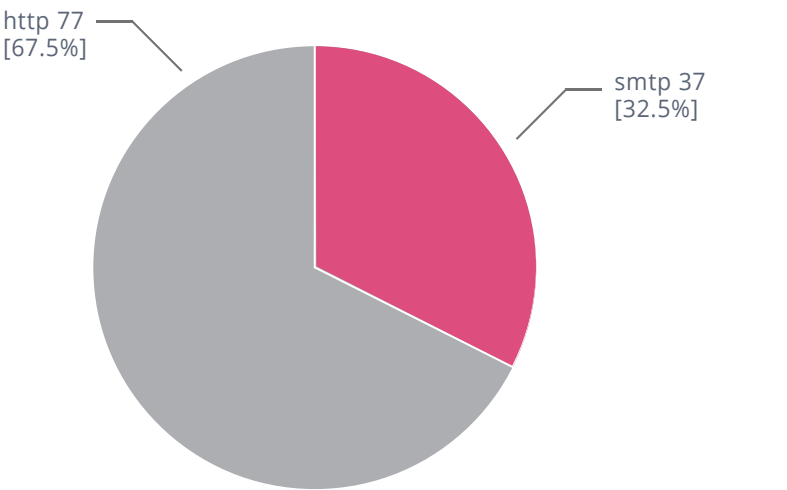
114

web data loss incidents

Top Data Types

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



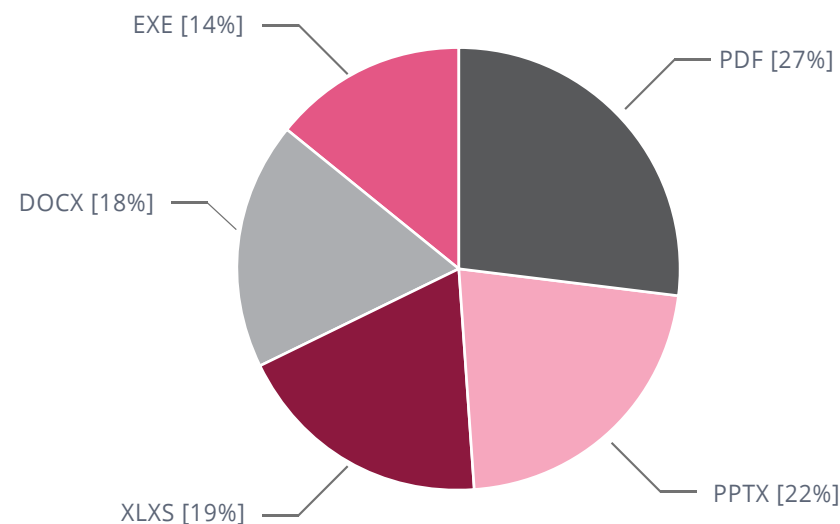
FILES UPLOADED TO CLOUD BASED WEB APPLICATIONS

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

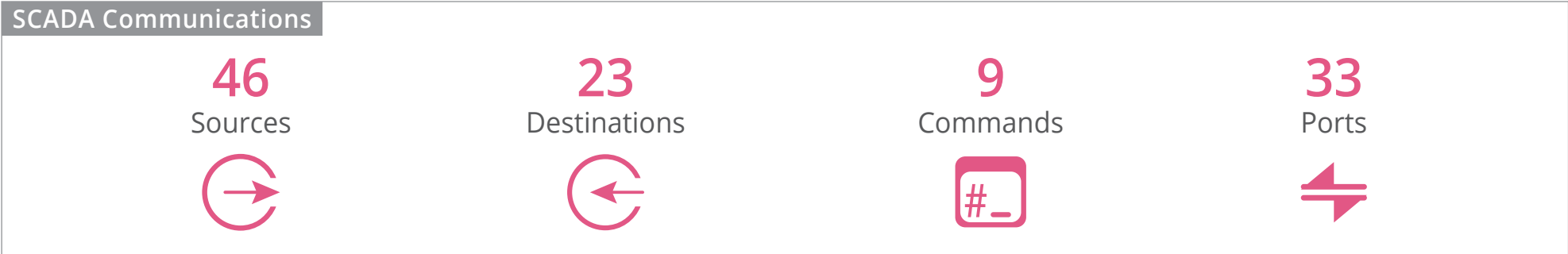
Site / Application Category	Site / Application	Uploaded Files	Number of Users	File Type
File Storage & Sharing Applications	Dropbox	7 Files	59 Users	.EXE, .PPTX, .PDF
	Hightail	4 Files	45 Users	.DOCX, .PPTX
	Mendeley	4 Files	21 Users	.PDF, .XLSX
	Google Drive-web	3 Files	13 Users	.EXE, .PDF
	Mega	3 Files	6 Users	.EXE
	Total: 7 Sites	24 Files	163 Users	
P2P File Sharing	BitTorrent Protocol	24 Files	65 Users	.DOCX, .PPTX
	SoulSeek	22 Files	55 Users	.PDF, .XLSX
	FileMp3.org	16 Files	43 Users	.PDF, PPTX
	P2P-Radio	9 Files	22 Users	.XLSX
	Sharebox	3 Files	10 Users	.PDF, .XLSX
	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	

File Types



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.

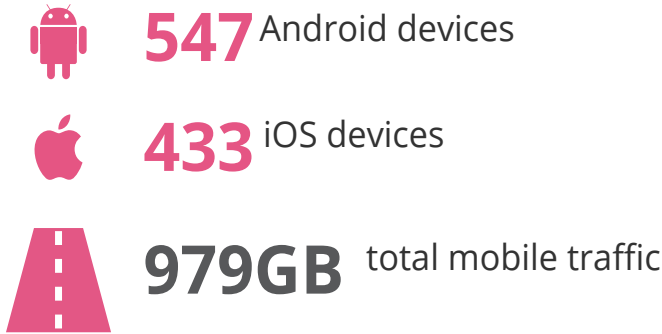


Top SCADA Protocols & Commands

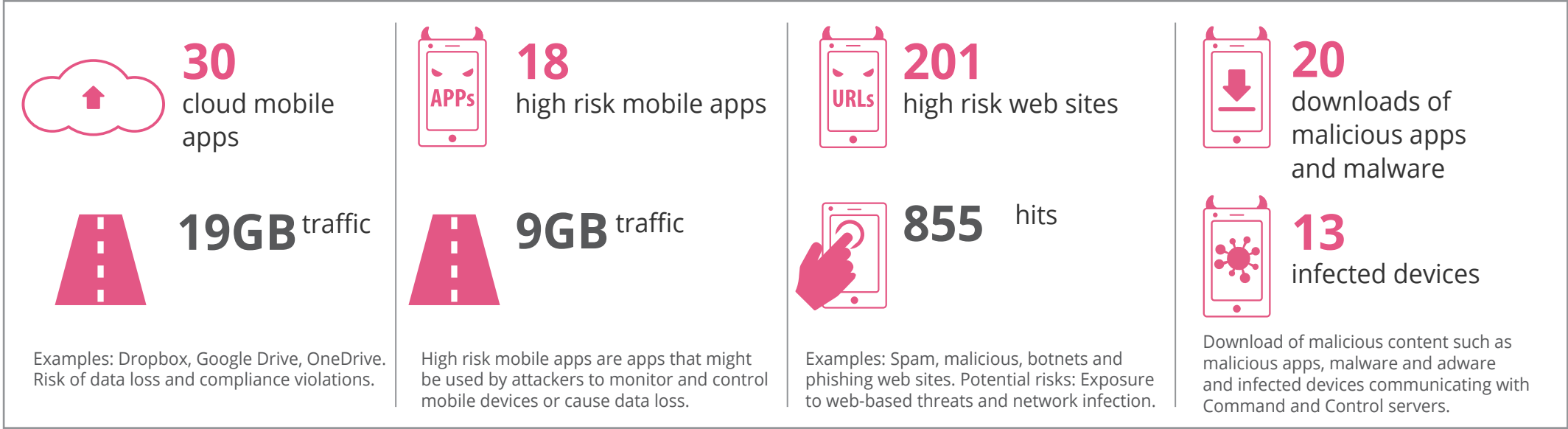
Protocol & Command	Transactions	Traffic
BACNet Protocol (Building Automation and Control Networks)	38	4.3GB
DNP3 Protocol - freeze and clear	21	123MB
EtherNet/IP	16	2.2GB
OPC UA - secure conversation message	2	71.0MB
DNP3 Protocol - immediate freeze	2	513MB
DNP3 Protocol	2	1.6GB
DNP3 Protocol - write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

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.



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



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

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 locations



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

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	58 devices	20 downloads	9 Files MD5

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

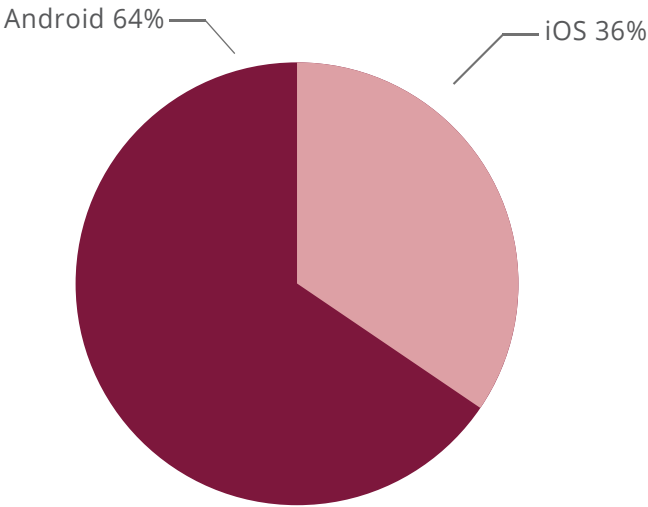
USAGE OF HIGH RISK MOBILE APPS

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	9 GB

Mobile devices



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

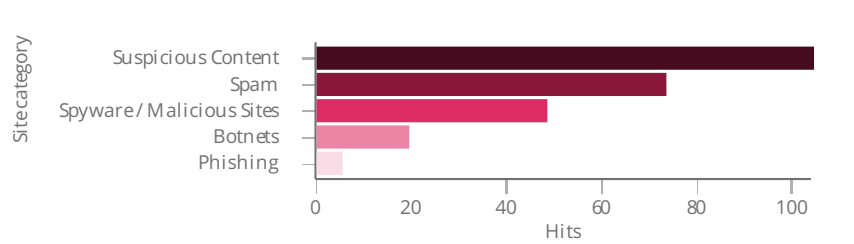
ACCESS TO HIGH RISK WEB SITES

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)

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

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
Total: 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

<div> 23 running high risk applications</div>	<div> 19 accessed high risk websites</div>
<div> 22 users accessed questionable, non-business related websites</div>	<div> 14 users involved in potential data loss incidents</div>

Endpoints Involved in Malware and Attack Incidents

<div> 34 infected with malware</div>	<div> 44 downloaded malware</div>	<div> 55 received email containing link to malicious site</div>
<div> 15 accessed a site known to contain malware</div>	<div> 22 servers attacked 23 clients attacked attacked endpoints</div>	

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.

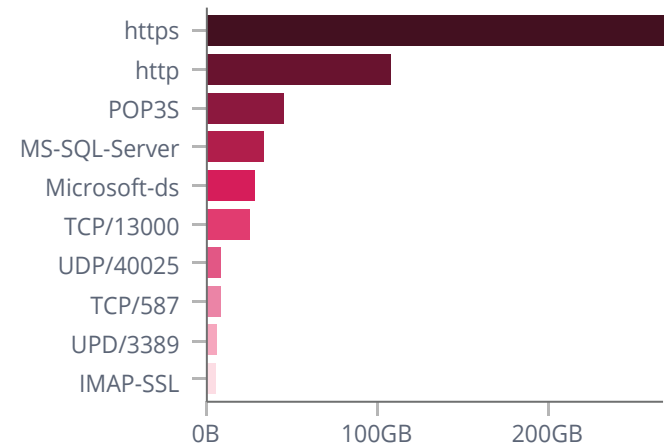
Top Applications/Sites (Top 30)

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.



CHECK POINT INFINITY

PREEMPTIVE CYBER SECURITY

Deploying security which is based on detection and followed by remediation is costly and inefficient, since it allows attackers to infiltrate 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®
SOFTWARE TECHNOLOGIES LTD.

SECURITY CHECKUP

THREAT ANALYSIS REPORT