INFONALIGY
Security Today for Tomorrow's Threats

SECURITY CHECKUP

THREAT ANALYSIS REPORT

Date:

Prepared for:

Prepared by:

Analysis duration:
Analysis Network Security:
Gateway version:
Security device:

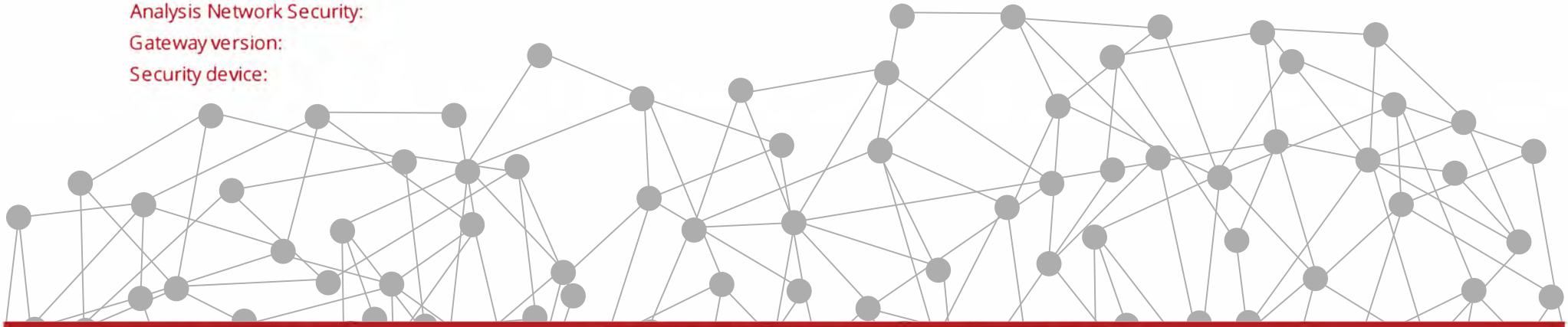


Table of Contents

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 Infonaligy 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.

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	4 Computers	13	Spain Italy
Total: 10 Malware Families	**287 Infected Computers**	**4,596**	**13 Countries**

Command & Control Locations

* Infonaligy'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.

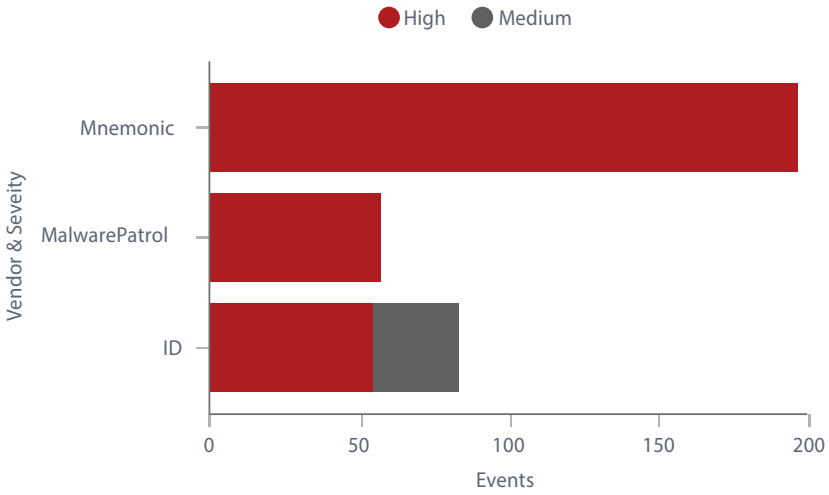
EXTENDED MALWARE INCIDENTS (INFONALIGY THREATCLOUD INTELLISTORE)

Malware threats were detected by extended security intelligence feeds (via Infonaligy 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 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



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**

* Infonaligy'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

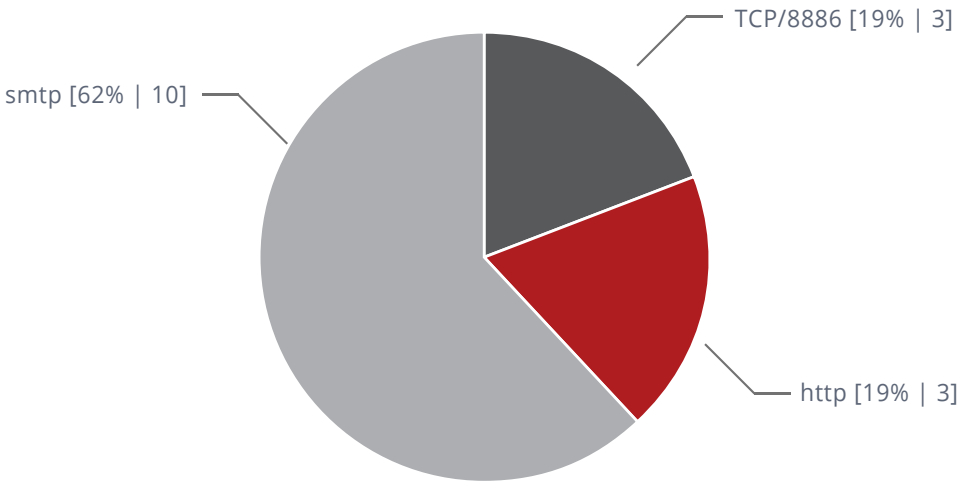
MALWARE DOWNLOADS (KNOWN MALWARE)

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	Downloaded 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



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.

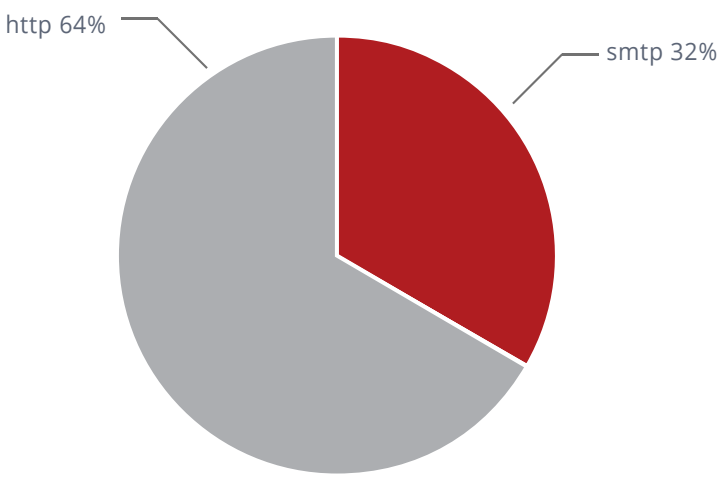
18.5K
total files scanned

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) Malware signature matched (Trojan.Win32.Generic.T.kbvx) Unexpected Process Crash	2	09831c2420848703 26865966037ea68f	smtp
0802_41.xls	Behaves like a known malware (Generic.MALWARE.6c6c) Malicious Filesystem Activity Malicious Registry Activity 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 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**

Download by Protocol



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

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 URLs by copying and pasting them into VirusTotal online service at www.virustotal.com

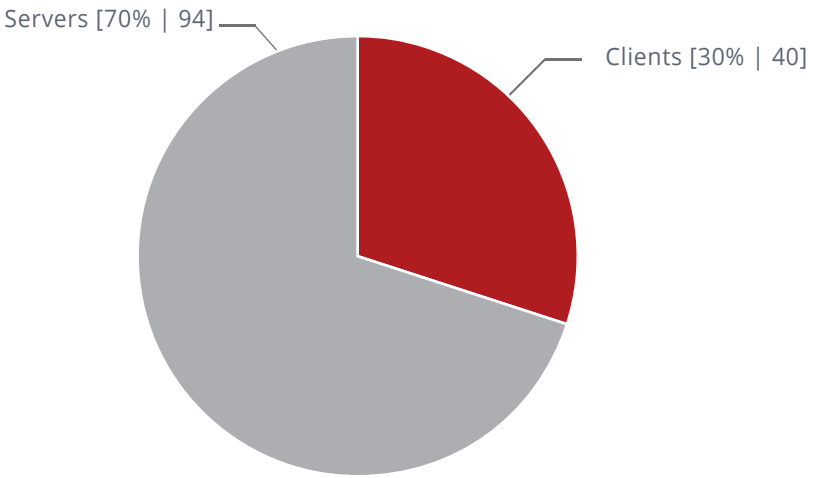
ATTACKS AND EXPLOITED SOFTWARE VULNERABILITIES

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 these events.

Attacks on Clients (Top 10 Attacks)

Attack Name	CVE	Attacked 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	265
Total: 5 Attacks		**94 Attacked Computers**	**594 Attackers**		**4,884 Attacks**

Attacked Targets



Attacks on Servers (Top 10 Attacks)

Attack Name	CVE *	Attacked Computer	Attackers	Severity	Number of Attacks
Microsoft SCCM Reflected Cross-site Scripting (MS12-062)	CVE-2012-2536	13	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: 9 Attacks		**40 Attacked Servers**	**265 Attackers**		**7,182 Attacks**

* For more information on specific CVE, search on MITRE's CVE search page (www.cve.mitre.org/cve/cve)

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	70.4K	13.3MB
attack types	total attacks	bandwidth utilization

Top 5 DDoS Attacks

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

Top Source Countries

Source Country	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**

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

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 (Top 5 Categories)

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.

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

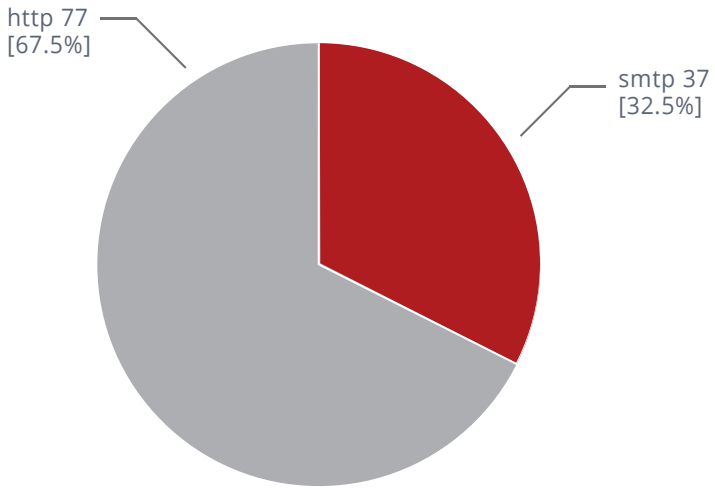
2 emails with data loss incidents

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



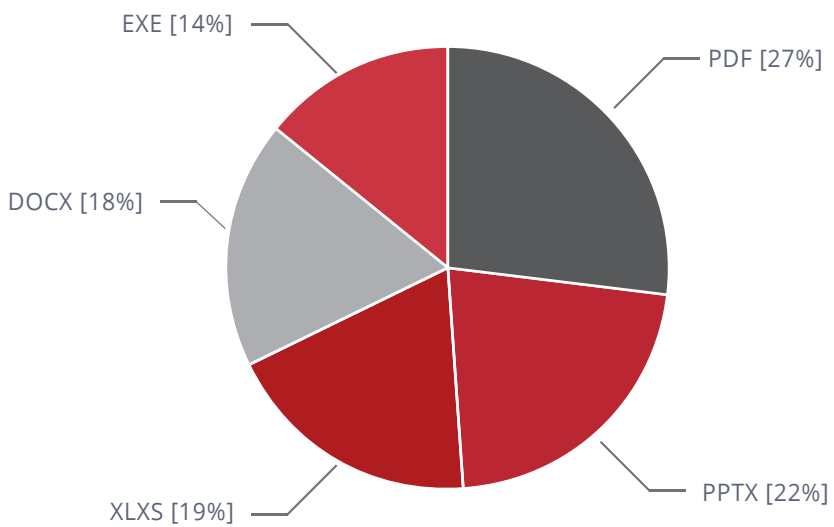
FILES UPLOADED TO CLOUD BASED WEB APPLICATIONS

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	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, .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**	

File Types



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	23	9	33
Sources	Destinations	Commands	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	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**

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

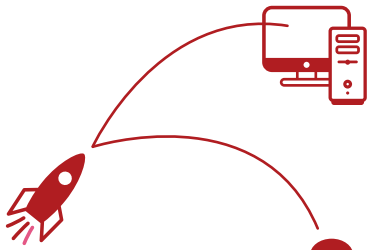
Endpoints Involved in Malware and Attack Incidents

34
infected with malware

44
downloaded malware

55
received email containing link to malicious site

15
accessed a site known to contain malware



22 servers attacked

attacked endpoints

23 clients attacked

BANDWIDTH UTILIZATION BY APPLICATIONS & WEBSITES

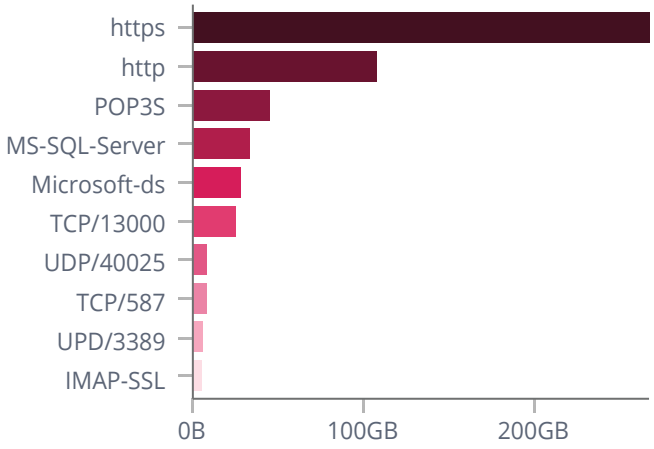
An organization's network bandwidth is usually utilized by a wide range of web applications and sites used by employees. Some are business related and some might not be business related. Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available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



About Infonaligy

For over 15 years, Infonaligy Partners has facilitated companies of all sizes in aligning technology with their business objectives.

The company provides clients with top-tier technology solutions, enabling them to increase security, reduce risk, and achieve greater operational value.

The team has the depth of knowledge, experience and resources to ensure clients' IT environments are efficient, protected, and well maintained. Whether it's Managed IT, Unified Communications, or Managed Security Services offerings, the Infonaligy team works to bring the best possible client experience to each engagement.

CORPORATE HEADQUARTERS

United States
550 Watters Creek Blvd. Suite 130, Allen
Texas, 75013 United States.

Please contact us for more information and to schedule your on-site assessment:

Within the US: 1-800-985-1365

Local in Dallas: 1-469-619-9474

INFONALIGY
Security Today for Tomorrow's Threats

www.infonaligy.com