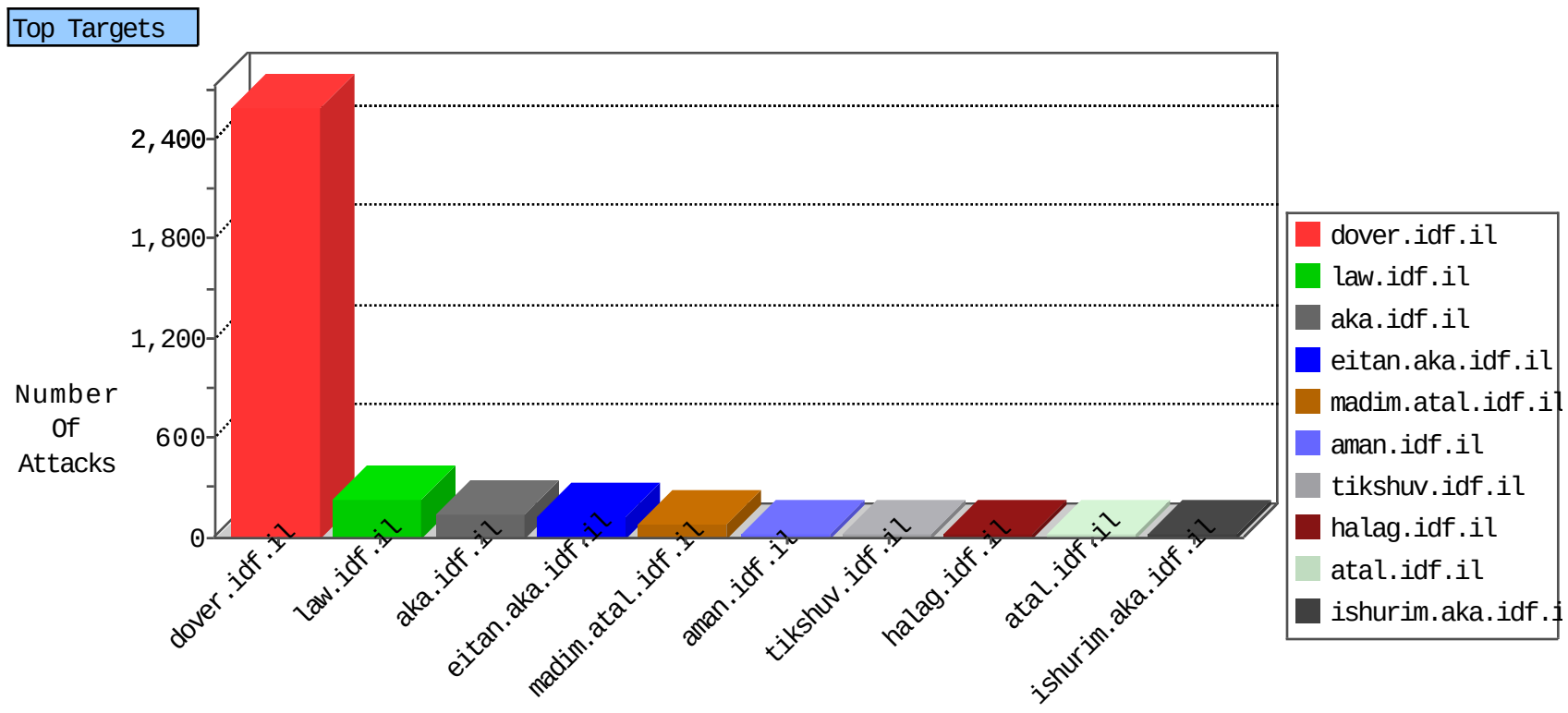
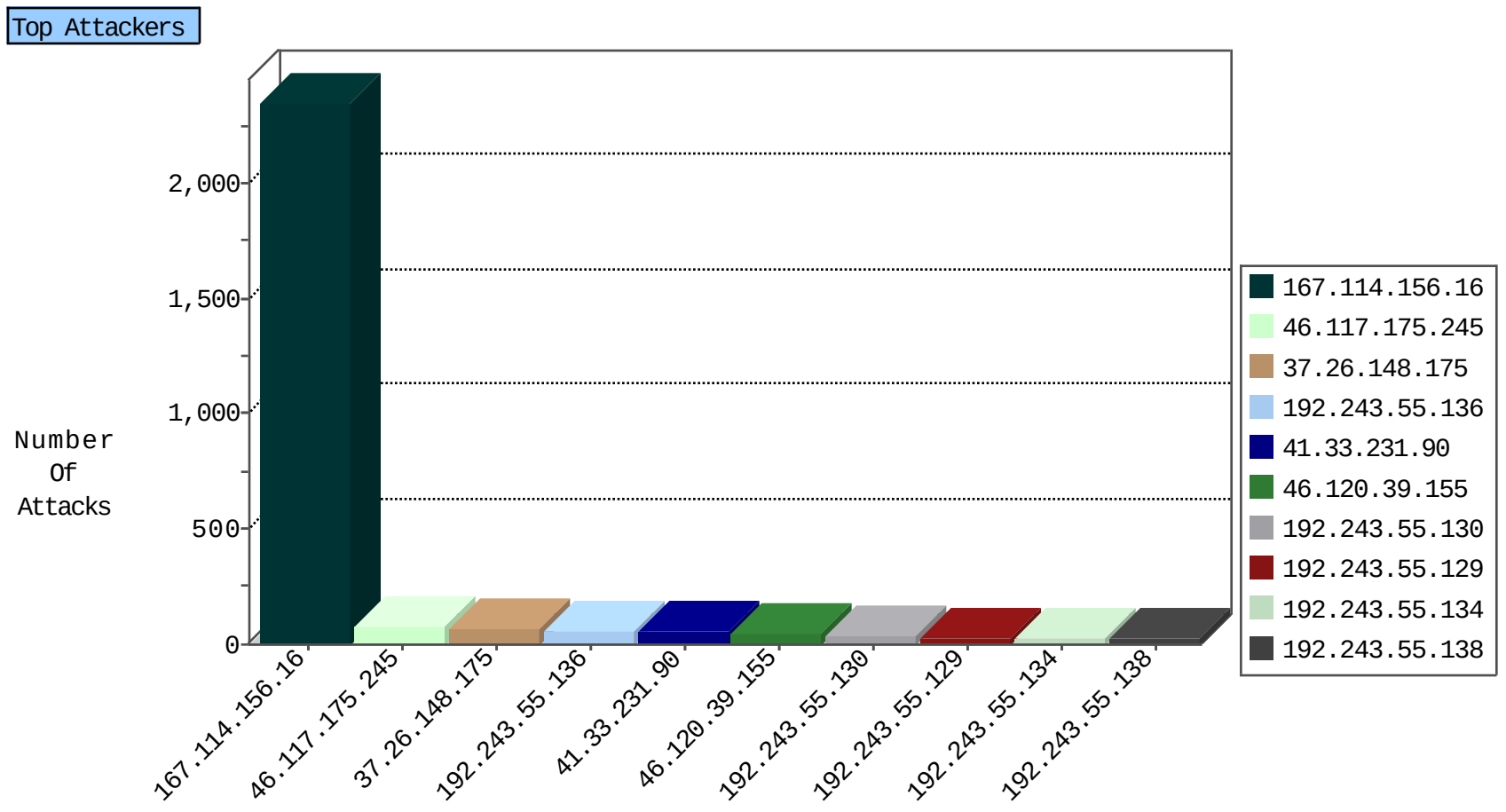
04-23-2016-14:04:03 to 04-23-2016-15:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-23-2016-14:04:03 to 04-23-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5674
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1544
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	524
149.50.15.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
1.234.27.16	Korea, Republic of	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
104.238.135.152	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
183.60.48.25	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-23-2016-14:04:03 to 04-23-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.194.92	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	3

04-23-2016-14:04:03 to 04-23-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.194.92	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
37.26.148.175	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
23.125.172.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
1.234.27.16	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
1.234.27.16	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
23.125.172.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.178.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
13.92.178.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
1.234.27.16	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
1.234.27.16	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
104.219.234.3	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

04-23-2016-14:04:03 to 04-23-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1349
46.117.175.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
46.120.39.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.13.218	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.43.73.91	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
31.154.171.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.111.70.10	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
41.232.105.12	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
66.87.116.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.90.122.239	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.90.122.239	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.96.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.122.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.250.129.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.174	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
177.231.218.59	Mexico	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.11.89	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
177.231.218.59	Mexico	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
177.231.218.59	Mexico	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-23-2016-14:04:03 to 04-23-2016-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
213.8.204.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	6
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.27.106.60	Block	4
46.121.144.142	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.144.142	Block	3
109.253.224.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.28.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
109.65.12.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
109.253.227.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/shared/clientscripts/mobile.js	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Malformed URL __atuvc=1	Block	1
109.253.141.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.93.170	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
176.13.13.218	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
91.135.111.85	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/grid.css	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method bsbt; in URL __atuvc=1	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
177.231.218.59	Mexico	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL [[#19]]û„‹y.´."-w[[#1]]¸[[#20]][[#16]][[#26]]zl¿Ù	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
107.150.46.38	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/900-he/אגף הטכנולוגי ה והלוגיסטיקה.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.253.224.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
85.64.2.183	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Malformed URL [[#19]]û„‹y.´."-w[[#1]]¸[[#20]][[#16]][[#26]]zl¿Ù	Block	1
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
46.121.144.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
89.105.158.229	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/story.aspx	Block	1
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
185.27.106.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.19.85.230	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvs=571b569f97d0ddc9000	Block	1
109.65.86.60	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/webresource.axd	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	NULL Character in Method	Block	1
5.28.172.123	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Abnormally Long Request method	Block	1
91.135.111.85	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 91.135.111.85	Block	1

04-23-2016-14:04:03 to 04-23-2016-15:04:03