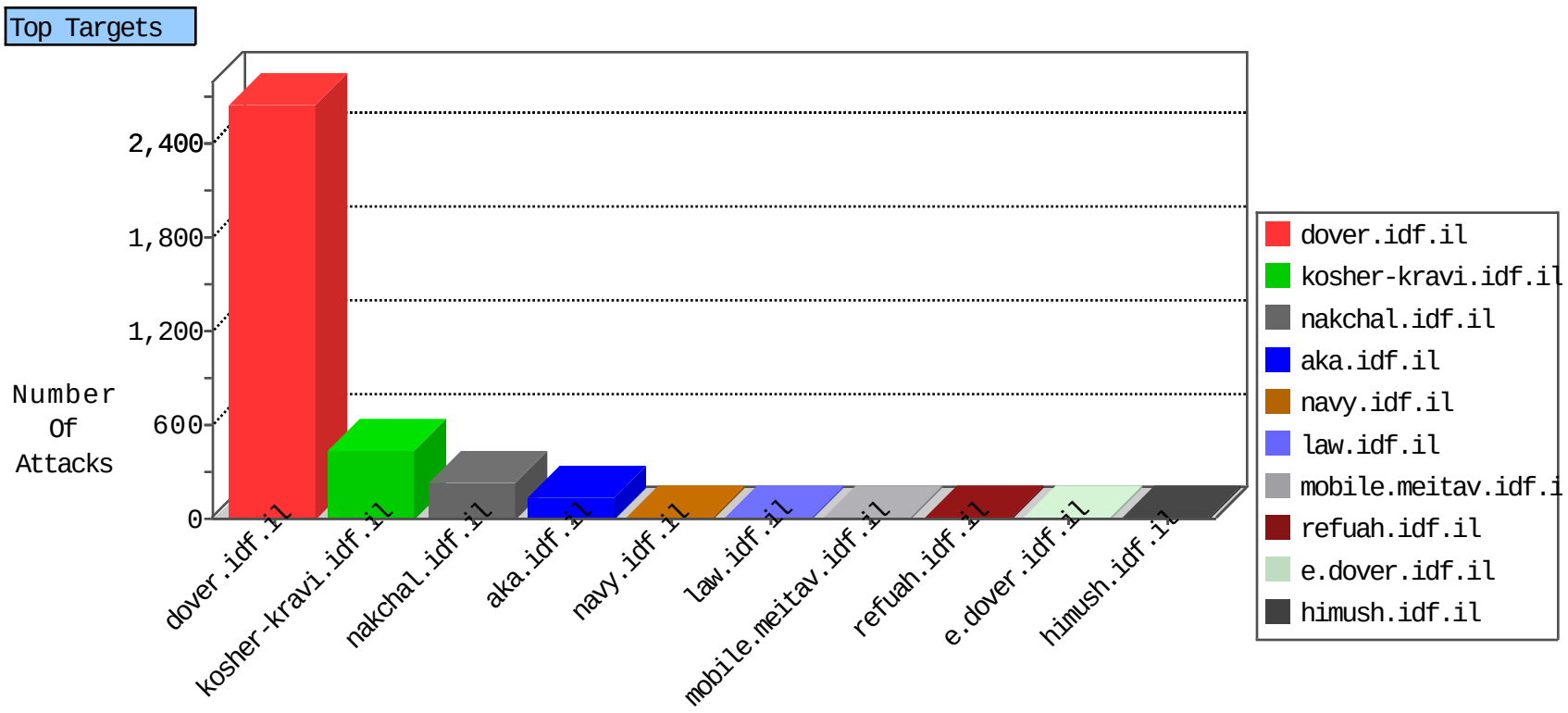
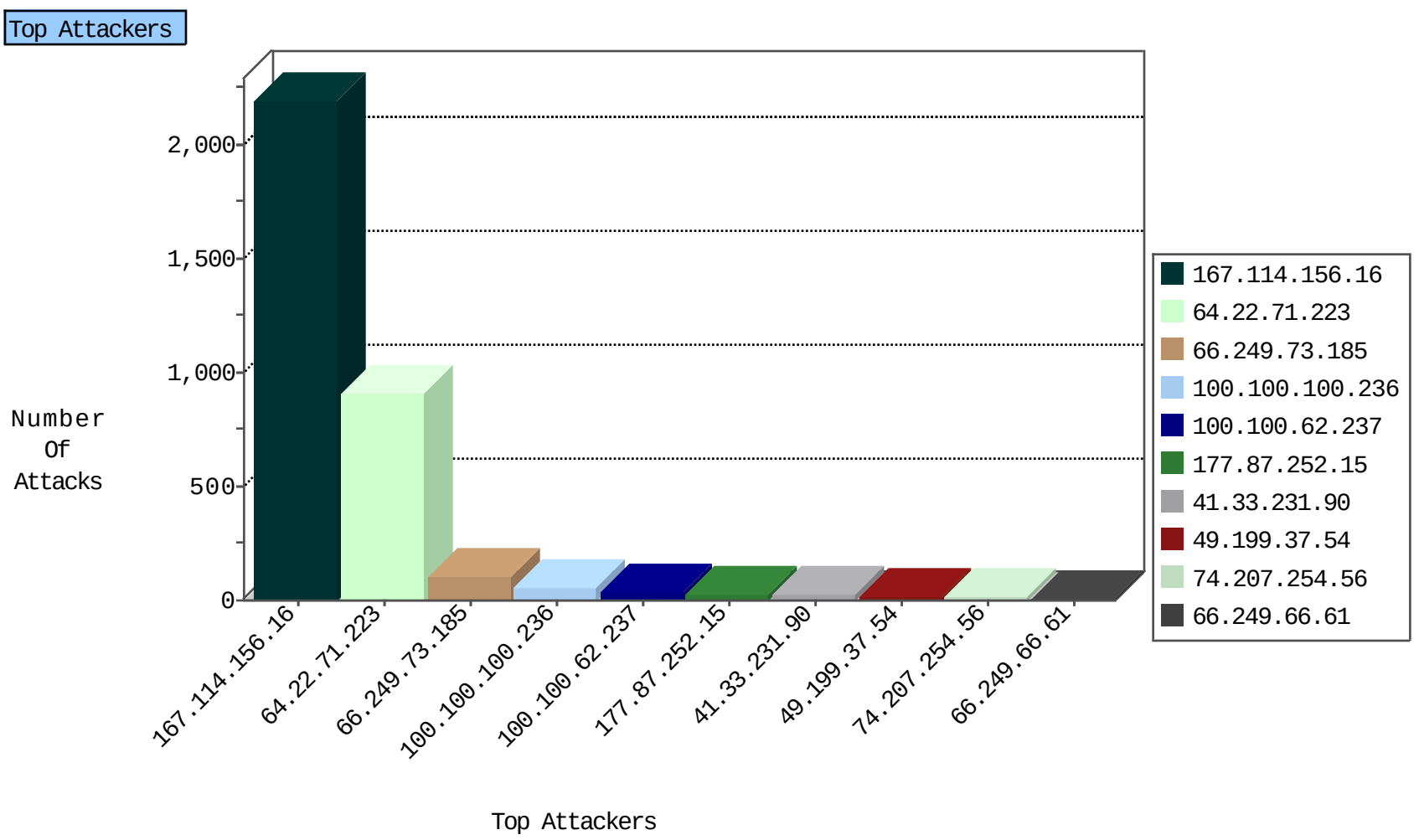
11-27-2015-03:04:08 to 11-27-2015-04:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015-03:04:08 to 11-27-2015-04:04:08

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	DOS-Tool-SwitchbladG	dest-reset	3300
64.22.71.223	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	4
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
177.87.252.15	Brazil	147.237.77.235	sviva.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
183.206.182.143	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
153.31.160.5	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
203.93.211.13	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
106.4.33.17	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
122.227.57.94	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

11-27-2015-03:04:08 to 11-27-2015-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-27-2015-03:04:08 to 11-27-2015-04:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.87.252.15	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
177.87.252.15	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Potential SSH Scan	2
177.87.252.15	147.237.77.205	Brazil	prisha.idf.il	ET SCAN Potential SSH Scan	1
118.71.153.234	147.237.77.216	Vietnam	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
177.87.252.15	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	1
118.71.153.234	147.237.77.74	Vietnam	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
177.87.252.15	147.237.76.148	Brazil	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
109.251.56.171	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.252.15	147.237.76.42	Brazil	refuah.idf.il	ET SCAN Potential SSH Scan	1
77.109.38.223	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.252.15	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
77.109.38.223	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.179	Australia	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
177.87.252.15	147.237.72.217	Brazil	e.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.252	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.176.210	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.0.15	Brazil	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
118.71.153.234	147.237.77.176	Vietnam	matpash.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
177.87.252.15	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.251.56.171	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.252.15	147.237.76.86	Brazil	navy.idf.il	ET SCAN Potential SSH Scan	1
88.132.80.230	147.237.76.30	Hungary	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.109.38.223	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
177.87.252.15	147.237.76.30	Brazil	himush.idf.il	ET SCAN Potential SSH Scan	1
51.255.47.120	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
210.50.197.154	147.237.77.179	Australia	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
177.87.252.15	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
198.23.176.210	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
177.87.252.15	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

11-27-2015-03:04:08 to 11-27-2015-04:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.22.71.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	245
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	106
100.100.100.236		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
100.100.62.237		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
49.199.37.54	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.4.65		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.168.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.57.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.137	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
174.129.237.157	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.221.229.96	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
110.240.123.83	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
199.30.25.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
85.250.252.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.87.116.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.248.205.225	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.139	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.37.223.60	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
64.22.71.223	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.69	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.134.127.108	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.114	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.7.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.81	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
197.134.127.108	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
49.199.37.54	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.37.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
118.202.25.224	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
216.218.206.114	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.7.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
42.62.74.74	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.82	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
100.100.14.183		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
197.134.127.108	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
64.125.239.14	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.195.54.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.33.32.25	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.138	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.37.223.60	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

11-27-2015-03:04:08 to 11-27-2015-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.22.71.223	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 64.22.71.223	Block	423
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	184
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17558.jpg	Block	4
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	4
64.22.71.223	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	3
64.22.71.223	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
5.107.127.70	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
74.207.254.56	United States	147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	1
114.97.54.36	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1356-he/cogat.aspx/trackback/	Block	1
74.207.254.56	United States	147.237.77.233	atal.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	1
46.116.106.18	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
74.207.254.56	United States	147.237.0.15	kosher-kravi.idf.i	Abnormally Long Request request version	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
176.73.193.168	Georgia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/2690.jpg	Block	1
108.253.80.158	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.107.127.70	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
212.199.136.107	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
74.207.254.56	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version + "?SearchText=" + escape($(" HTTP/1.1	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
136.243.24.148	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
95.175.97.229	Finland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.116.106.18	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 46.116.106.18	Block	1
74.207.254.56	United States	147.237.0.15	kosher-kravi.idf.i	Illegal HTTP Version + "?SearchText=" + escape($(" HTTP/1.1	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar	Block	1
176.73.193.168	Georgia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/2431.jpg	Block	1
108.253.80.158	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
64.22.71.223	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
74.207.254.56	United States	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.61	Block	1
207.46.13.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/	Block	1
64.22.71.223	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/usercontrols/headerupper	Block	1
141.212.122.64	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.117.123.176	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.117.123.176 (Open Mode)	None	1
74.207.254.56	United States	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
197.35.207.202	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/2801.jpg	Block	1
64.22.71.223	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
109.65.27.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.106.18	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
74.207.254.56	United States	147.237.77.216	dover.idf.il	Illegal HTTP Version + "?SearchText=" + escape($(" HTTP/1.1	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/halochamim	Block	1

11-27-2015-03:04:08 to 11-27-2015-04:04:08