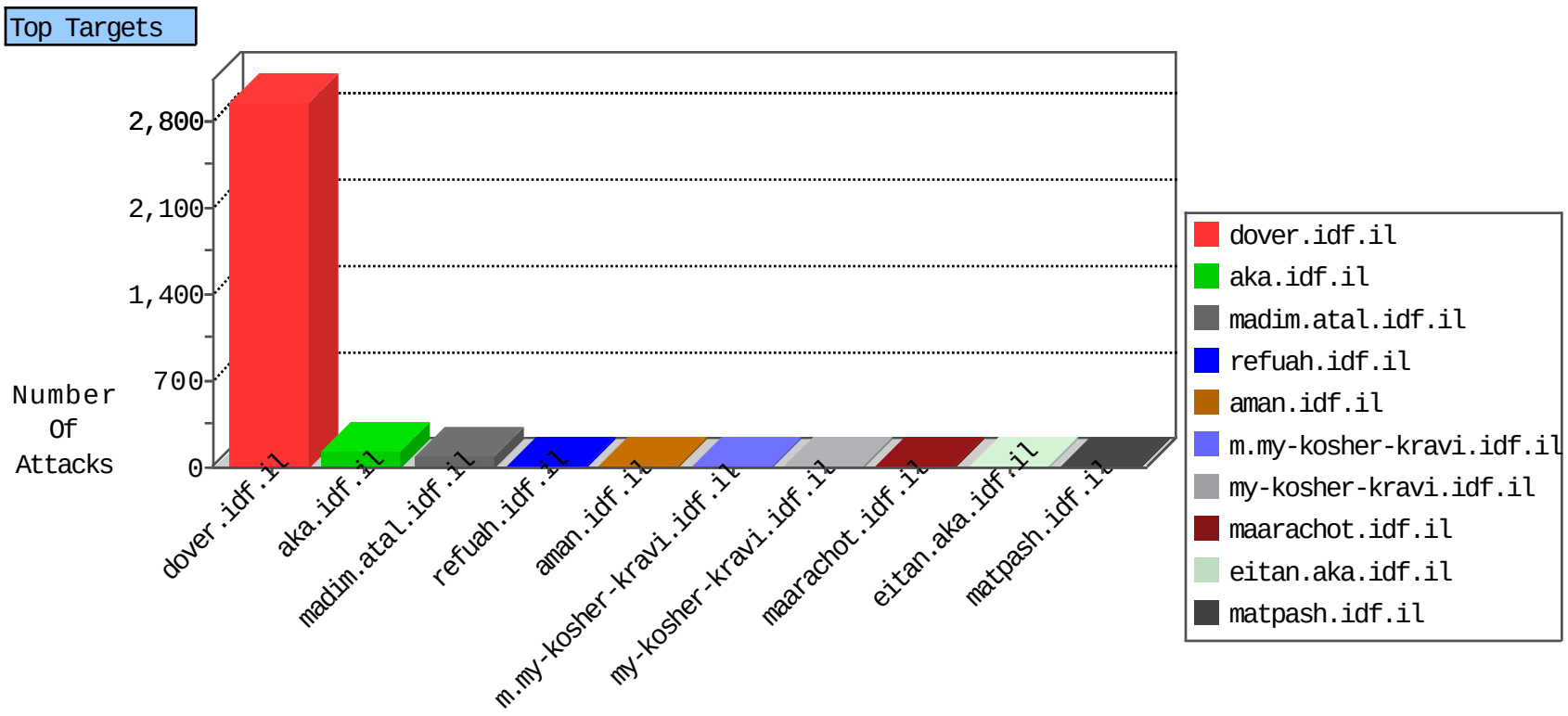
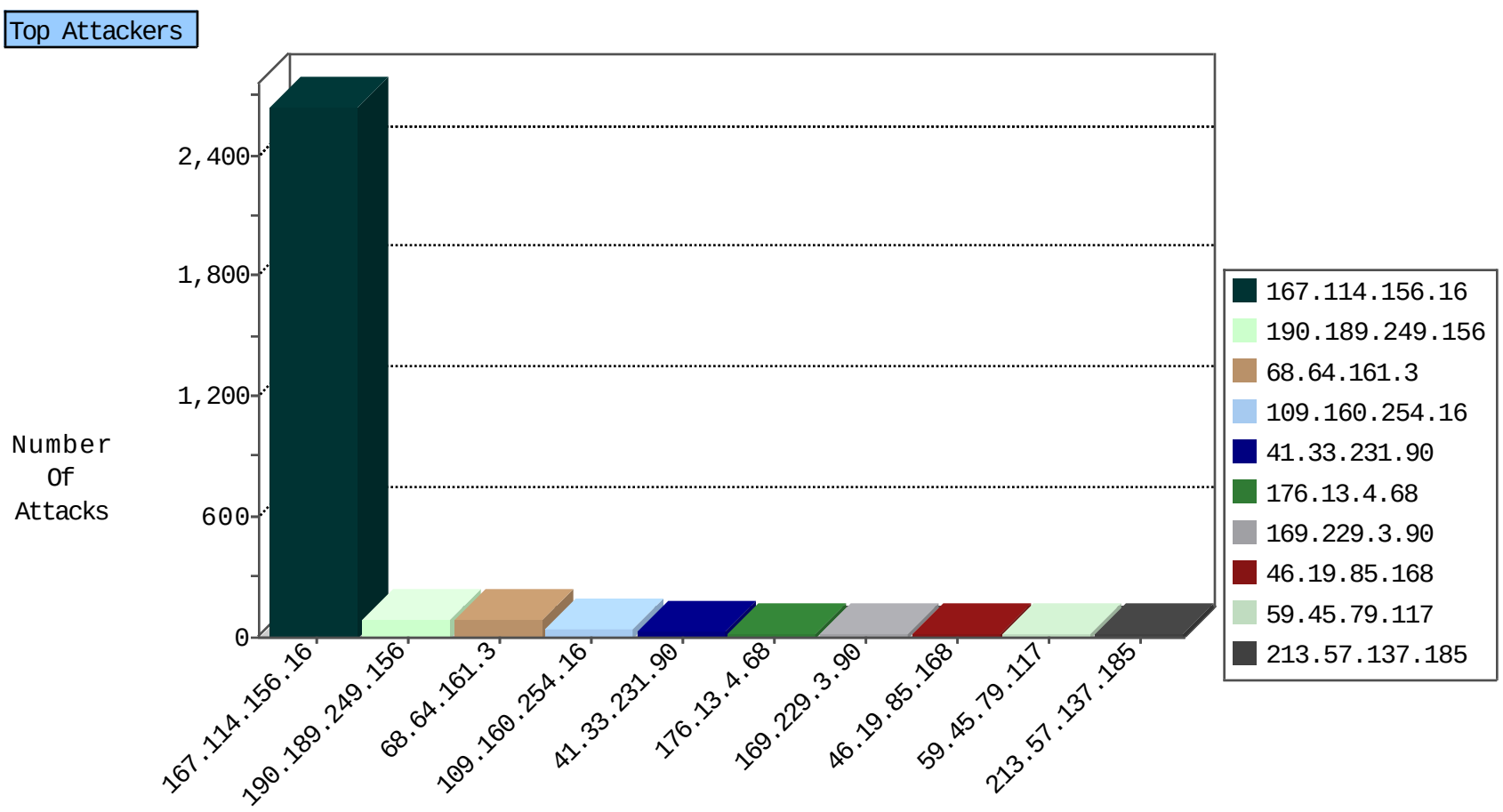
12-05-2015-10:04:07 to 12-05-2015-11:04:07

IDF Under Attack Daily Report





12-05-2015-10:04:07 to 12-05-2015-11:04:07

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	3337
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1249
149.88.142.57	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	42
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
10.0.0.3		147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
202.112.51.96	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
64.246.161.190	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
104.233.78.45		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

12-05-2015-10:04:07 to 12-05-2015-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.64.161.3	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
68.64.161.3	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
203.87.119.8	Australia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

12-05-2015-10:04:07 to 12-05-2015-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
81.212.109.229	147.237.76.177	Turkey	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
81.212.109.229	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
81.212.109.229	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 3072	1
62.212.73.196	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
120.26.205.111	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
120.26.205.111	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
120.26.205.111	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.218.246.103	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
81.212.109.229	147.237.76.199	Turkey	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
81.212.109.229	147.237.76.42	Turkey	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
81.212.109.229	147.237.0.33	Turkey	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
120.26.205.111	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
120.26.205.111	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
120.26.205.111	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
81.212.109.229	147.237.77.216	Turkey	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1

12-05-2015-10:04:07 to 12-05-2015-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.94.161.14	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.117	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.81.14.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.18.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.145.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.137.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
213.57.137.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.137.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.108.206.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
64.246.161.190	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
212.143.142.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.192.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.60	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.132.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.3.144.54	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.201.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.137.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.132.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.68.46.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.217.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.99.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
77.125.151.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.132.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
169.229.3.90	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.121.192	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.142.201.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.12.147.196	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.121.192	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.22.131.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.12.147.196	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
169.229.3.90	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
169.229.3.90	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.146.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-05-2015-10:04:07 to 12-05-2015-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.254.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
68.64.161.3	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.64.161.3	Block	31
176.13.4.68	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	14
149.78.58.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	8
176.13.4.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.206	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
68.64.161.3	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.54.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.9	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
84.109.17.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.81.14.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
176.13.13.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.64.161.3	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 68.64.161.3	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
2.54.180.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.145.35	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
176.228.188.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.155.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/sckjksdcfksdshitjfsl.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.94.161.14	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
212.116.187.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
176.13.13.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1065-he/dover.aspx	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.149.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.179.53.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
196.206.22.5	Morocco	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch	Block	1
109.64.18.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
46.120.156.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.108.157.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.20	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
176.13.13.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.64.161.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71861-he/maarachot.aspx	Block	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
23.254.243.17	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
85.250.0.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1
79.181.104.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
196.206.22.5	Morocco	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.220.156.103	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.20	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.8.204.20	Block	1
84.108.212.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.23.146	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1

12-05-2015-10:04:07 to 12-05-2015-11:04:07