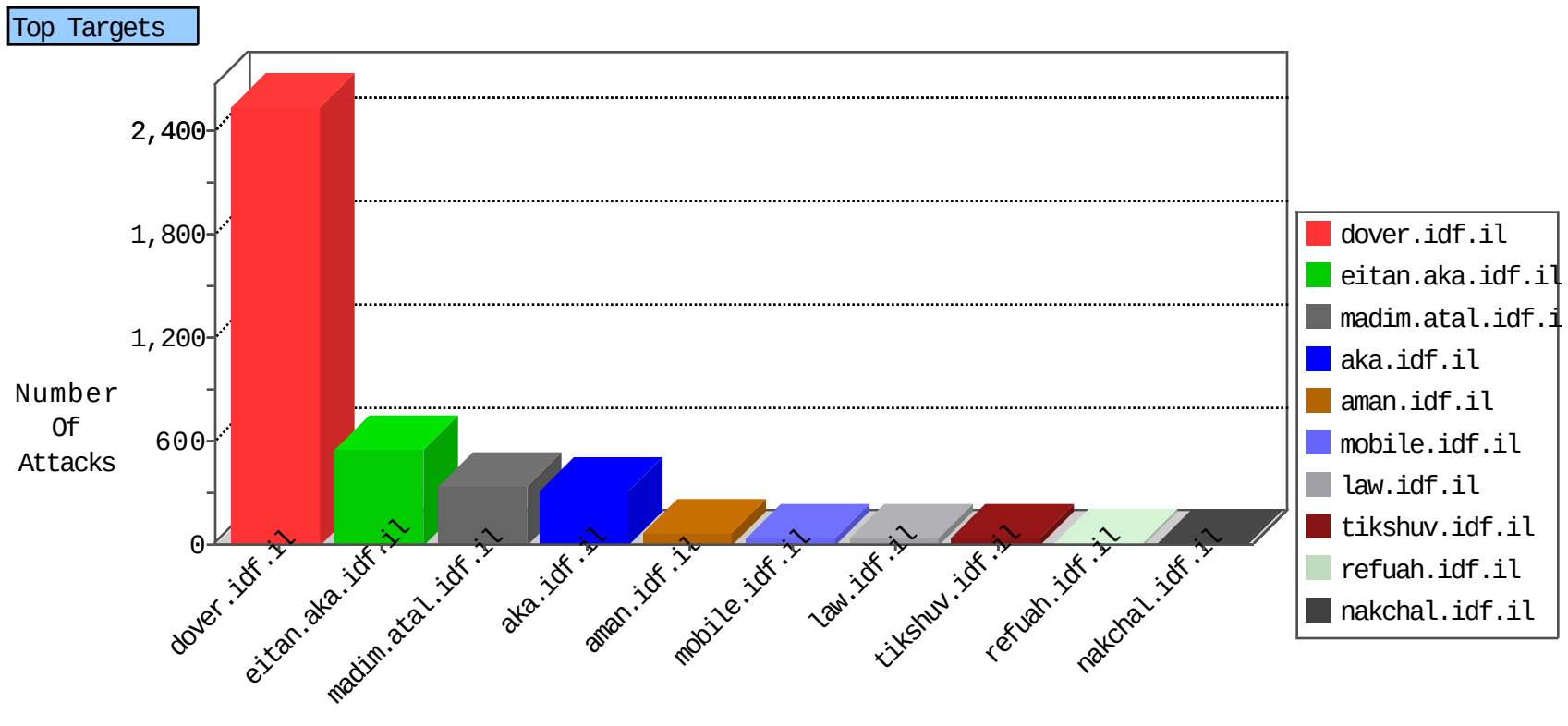
11-27-2015-17:04:02 to 11-27-2015-18:04:02

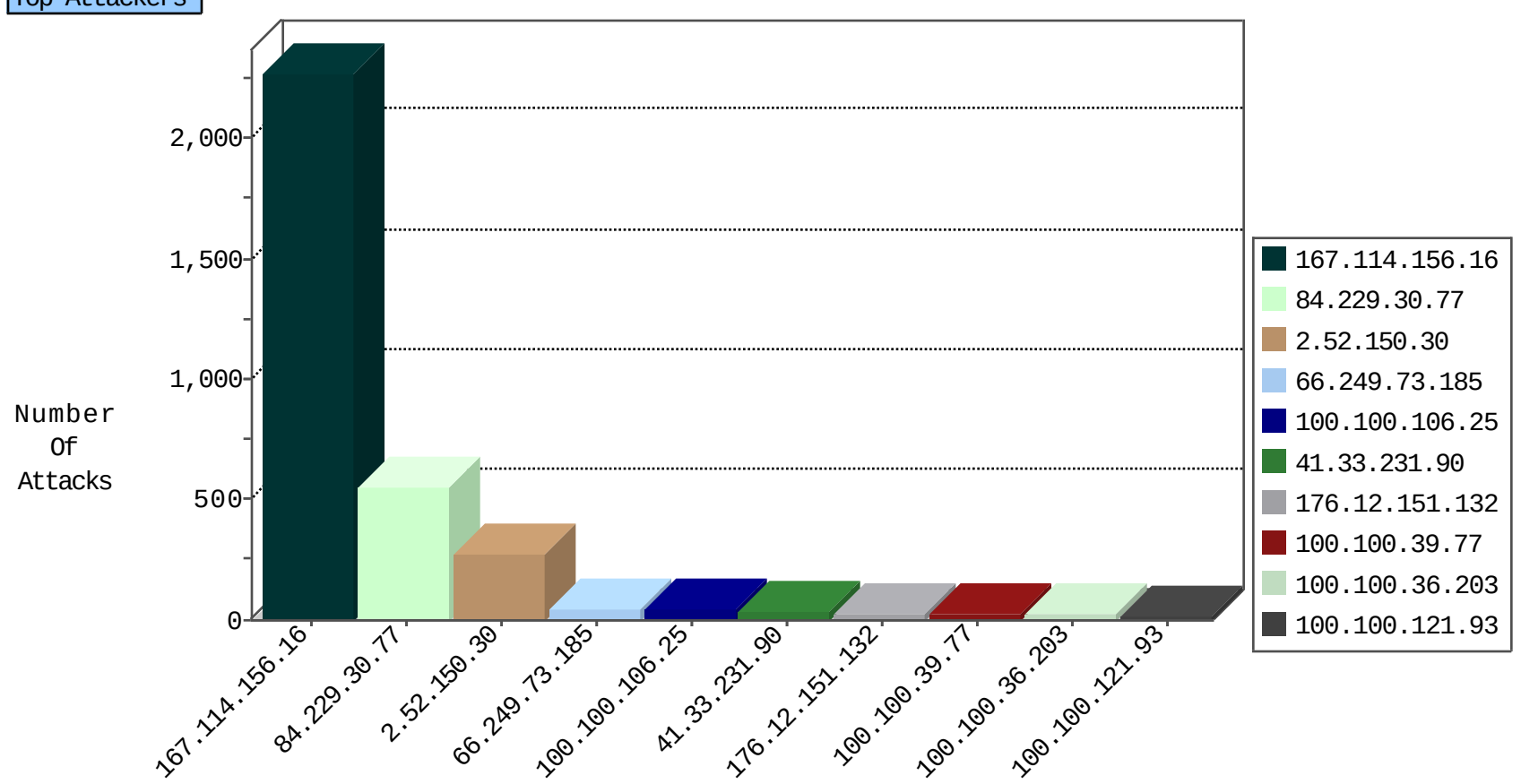
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-27-2015-17:04:02 to 11-27-2015-18:04:02

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	3282
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
77.74.34.204	Belarus	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

11-27-2015-17:04:02 to 11-27-2015-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-27-2015-17:04:02 to 11-27-2015-18:04:02

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
116.24.250.31	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.231	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
116.24.250.31	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
116.24.250.31	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
116.24.250.31	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
116.24.250.31	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.252	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
116.24.250.31	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.117.92.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.227.196.29	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
116.24.250.31	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
116.24.250.31	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
79.181.50.179	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
116.24.250.31	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
116.24.250.31	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
116.24.250.31	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
116.24.250.31	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.252	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.24.250.31	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
23.227.196.29	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.42.218	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP JBoss JMXInvokerServlet access attempt	1
23.227.196.29	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
95.22.80.208	147.237.8.28	Spain	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.24.250.31	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
74.208.229.197	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

11-27-2015-17:04:02 to 11-27-2015-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.229.30.77	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	507
66.249.73.185	United States	147.237.77.216	dover.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	32
100.100.106.25		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
100.100.39.77		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.121.93		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.36.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
100.100.106.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
100.100.45.4		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.92.200		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.117.81		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
100.100.48.159		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
24.114.83.248	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.116.125.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.173.151.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.24	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.224	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.179.91.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
79.179.52.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.52.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
173.252.89.52	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.36.203		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.142.227.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
100.100.39.77		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
37.142.227.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
173.252.89.57	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
84.111.37.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.172.172.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.212.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.182.146.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.81.175	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
100.100.125.75		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.65.4.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.6		147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.30.24.245	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
80.246.139.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.143.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.30.25.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
173.252.89.54	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
100.100.92.200		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.6.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

11-27-2015-17:04:02 to 11-27-2015-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	47
84.229.30.77	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.229.30.77	Block	44
176.12.151.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
31.154.10.107	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	6
84.108.97.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.106.227.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.49.241	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.49.241	Block	3
46.19.86.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.127.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	2
46.120.47.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.67.29.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
85.64.235.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1390	Block	2
109.66.30.143	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
176.13.7.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.73.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.151.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
149.78.228.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.38.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.34.82.10	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
40.77.167.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
149.88.127.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	2
2.54.43.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.68.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
109.64.28.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
31.215.35.15	United Arab Emirates	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
85.64.75.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.136.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.44.153	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	1
62.90.153.17	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1
109.186.13.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
109.65.183.183	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	1
79.176.200.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
207.46.13.87	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8890-he/navy.aspx	Block	1
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.50.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
176.13.5.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
132.64.142.38	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
8.37.70.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhhyunvaom6r4ixgbqtotzguy0d8jw	Block	1

11-27-2015-17:04:02 to 11-27-2015-18:04:02