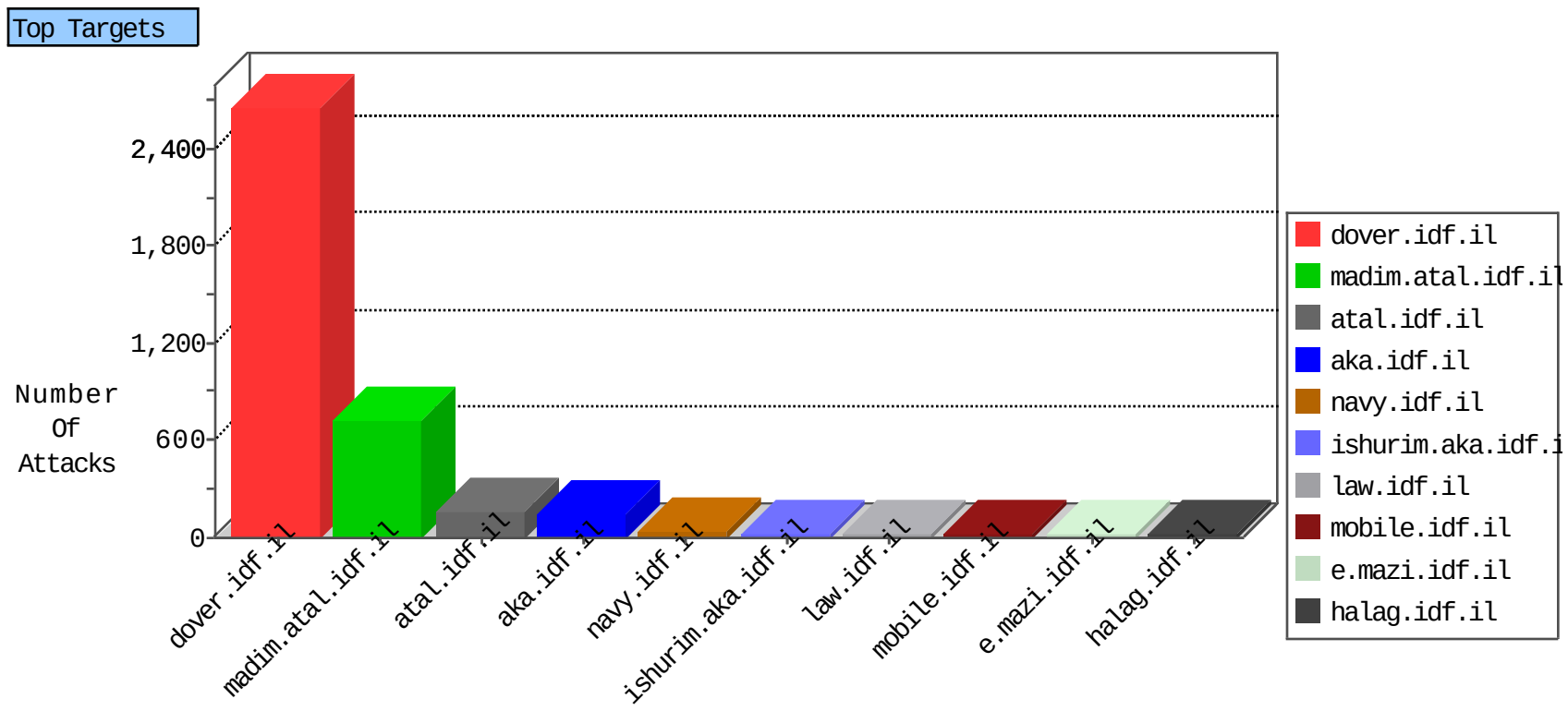
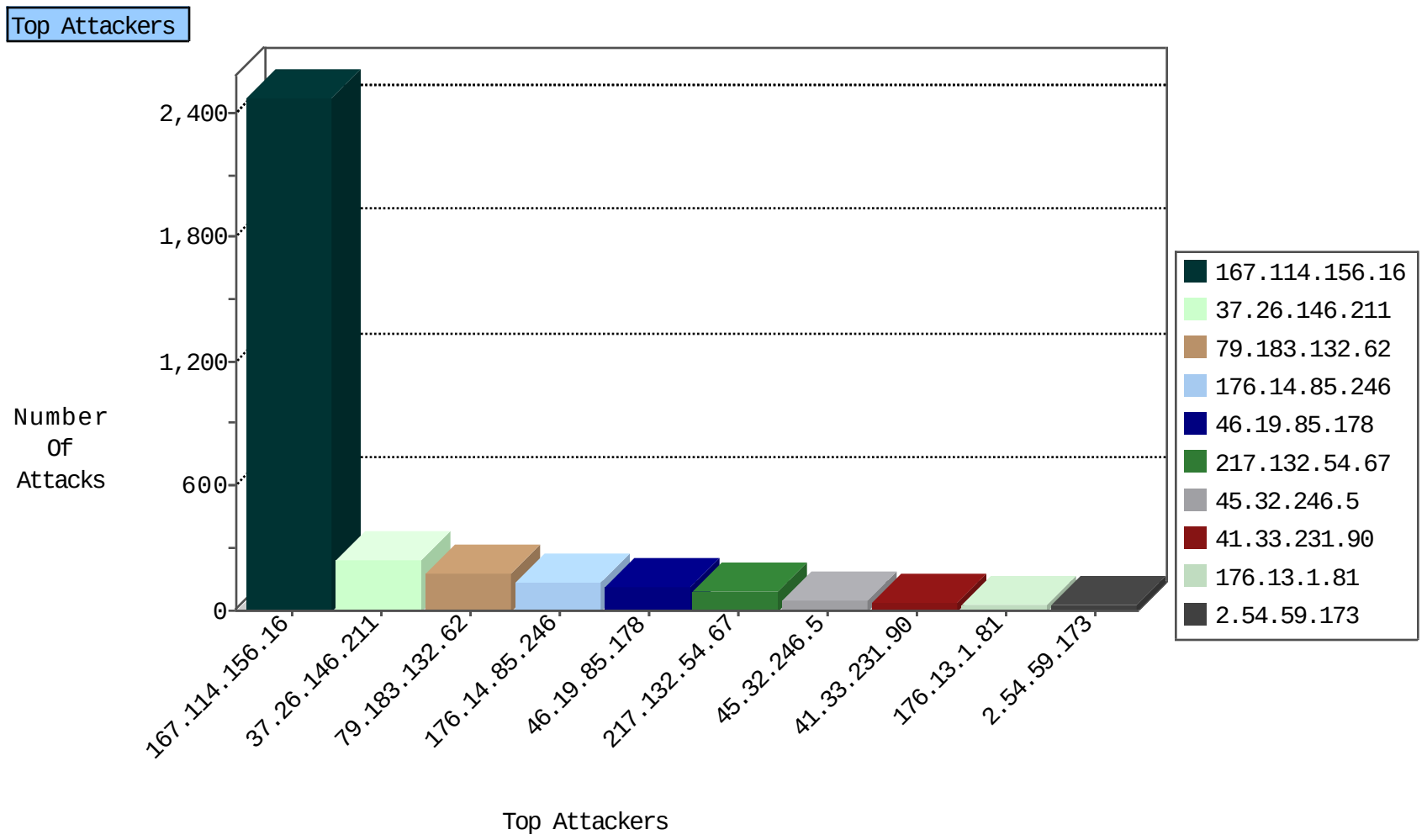
12-10-2015-08:04:04 to 12-10-2015-09:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-10-2015-08:04:04 to 12-10-2015-09:04:04

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	3403
45.32.246.5		147.237.77.74	law.idf.il	Invalid TCP Flags	drop	9
81.218.105.235	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.77.179	e.mazi.idf.il	Invalid TCP Flags	drop	1
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	1
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	1

12-10-2015-08:04:04 to 12-10-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.35.187.114	United States	147.237.77.234	halag.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
69.12.70.34	United States	147.237.0.34	tikshuv.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
52.33.106.123	United States	147.237.77.216	dover.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-10-2015-08:04:04 to 12-10-2015-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
12.139.41.189	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
117.25.155.164	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
93.93.218.250	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
83.205.150.17	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.120.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.202	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
183.82.98.215	147.237.76.34	India	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.246.5	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
166.63.125.149	147.237.76.176	United States	test.ncore.idf.i	ET SCAN NMAP -sS window 3072	1
2.54.24.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.25.155.164	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -f -sS	1
93.93.218.250	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.7.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.31.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.246.5	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -f -sS	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
45.32.246.5	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

12-10-2015-08:04:04 to 12-10-2015-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	136
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
141.0.15.203	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
79.178.123.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
185.32.179.89	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
132.74.213.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
132.74.213.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
217.132.54.67	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.32.246.5		147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.28.150.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.32.246.5		147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.135.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
45.32.246.5		147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
45.32.246.5		147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
212.199.57.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.120	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.120	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.139.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.50.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.132.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.177.162	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.120	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.17.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
173.243.112.148	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.179.7.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.221.236.249	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
217.132.5.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.153.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.179.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.40.18	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.43.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.246.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.14.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.41.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.27.89.59	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.74.213.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.67.132.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.211.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.241.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.211	Block	147
79.183.132.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
217.132.54.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
79.183.132.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
176.13.1.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.59.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
192.118.99.100	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.118.99.100	Block	8
79.183.132.62	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.183.132.62	Block	5
93.173.225.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
213.57.106.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
176.12.142.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
217.132.54.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
79.177.23.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.31.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.161.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.88.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-8890-he/dover.aspx	Block	1
109.160.248.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
52.35.187.114	United States	147.237.77.234	halag.idf.il	Multiple Illegal Byte Code Character in Method from 52.35.187.114	Block	1
79.178.123.99	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.255	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.75.30	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter subject in www.eitan.aka.idf.il/1105-en/eitan.aspx	None	1
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	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
52.33.106.123	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 52.33.106.123	Block	1
79.183.132.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
78.111.186.184	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.111.186.184	Block	1
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
110.159.80.80	Malaysia	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
95.108.158.191	Russian Federation	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
52.35.187.114	United States	147.237.77.234	halag.idf.il	Multiple NULL Character in Method from 52.35.187.114	Block	1
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	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