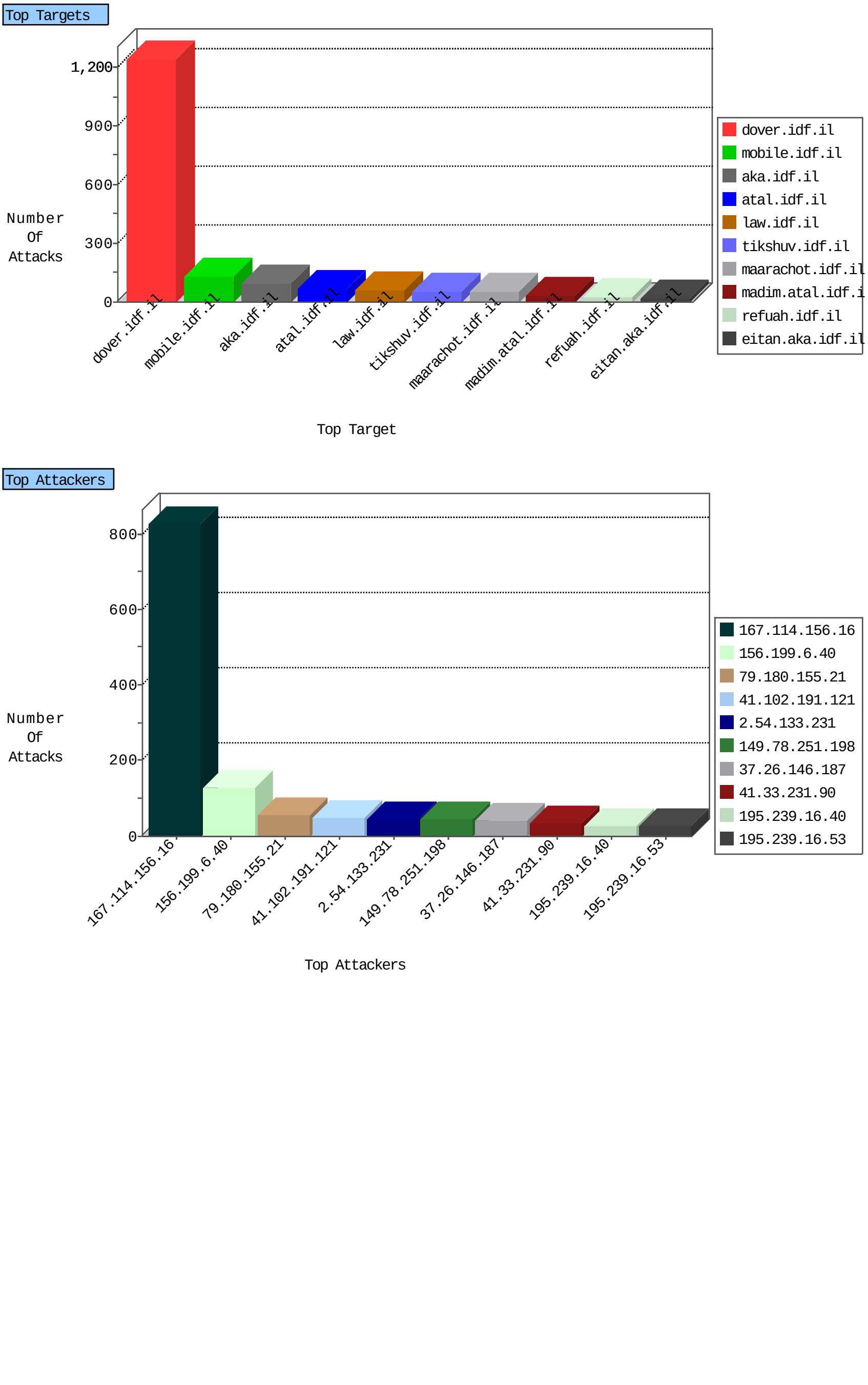
12-31-2015-23:04:01 to 01-01-2016-00:04:01

IDF Under Attack Daily Report



12-31-2015-23:04:01 to 01-01-2016-00:04:01

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	3809
79.180.59.236	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
109.67.183.51	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
2.52.32.106	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
211.14.251.225	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.212	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

12-31-2015-23:04:01 to 01-01-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-31-2015-23:04:01 to 01-01-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.40	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
192.198.94.252	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
61.240.144.64	147.237.77.233	China	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.209.49.224	147.237.76.30	Romania	himush.idf.il	ET SCAN Potential SSH Scan	1
12.139.41.189	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
188.209.49.224	147.237.0.19	Romania	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.39		mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.76.177	China	ncore.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
185.130.5.231	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
212.164.232.56	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
212.164.232.56	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
177.139.117.195	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.67.1.155	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
104.238.160.101	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
192.198.94.252	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
192.198.94.252	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
42.69.23.30	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.209.49.224	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
212.164.232.56	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
212.164.232.56	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
212.164.232.56	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
125.26.223.161	147.237.76.31	Thailand	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-31-2015-23:04:01 to 01-01-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
156.199.6.40		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	128
41.102.191.121	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
79.180.155.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
149.78.251.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
37.26.146.187	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
2.54.133.231	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
94.230.92.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
5.102.241.43	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
207.241.225.185	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	18
2.54.154.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.186.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.133.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.135.225	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.180.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.146.24	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.179	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
46.19.86.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.179	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.180.59.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.133.231	Israel	147.237.77.243	mobile.idf.il	SYN Attack		reject	5
2.52.32.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
96.224.13.26	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.133.40	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
207.46.13.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.119	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.26.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.0.171	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.117.24.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.0.171	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.133.231	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.97.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.3.147.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.181.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.172.135.28	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
2.54.133.231	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
2.54.131.194	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.188.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.254.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.180.155.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
95.86.122.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
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	2
46.117.24.145	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
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
185.32.179.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
2.54.154.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.26.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.37.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
176.12.140.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.54.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
93.172.2.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.128.6	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
80.230.7.165	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
114.97.59.23	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-he/cogat.aspx/trackback/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12801-h	Block	1
50.196.99.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
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	1
85.250.14.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
37.142.64.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.150.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.6.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.159.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
94.230.92.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.117.24.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.175.25.171	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.228.128.6	None	1
84.109.117.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.78.251.198	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/993/patzar.aspx	Block	1
87.69.100.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
40.77.167.88	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
213.151.39.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.214.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.3.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.7.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.198.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
31.13.110.127	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.228.93.1	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
156.199.6.40		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1