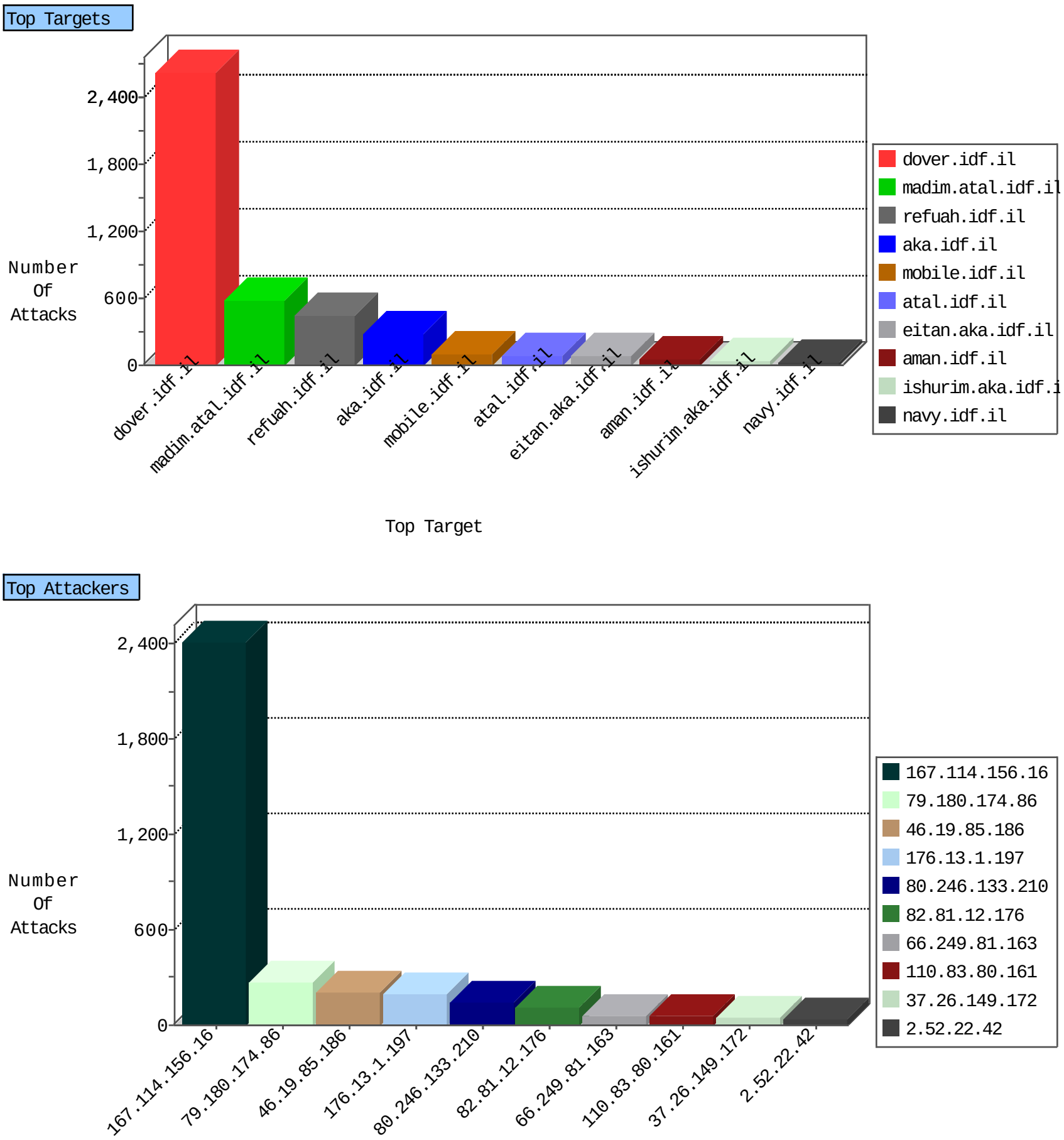
01-25-2016-08:04:09 to 01-25-2016-09:04:09

IDF Under Attack Daily Report



01-25-2016-08:04:09 to 01-25-2016-09:04:09

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	3049
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
8.37.237.250	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
82.145.33.11	United Kingdom	147.237.76.200	eitan.aka.idf.il	Block_Ip_Web_In	drop	1
117.79.146.2	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

01-25-2016-08:04:09 to 01-25-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.83.80.161	China	147.237.77.74	law.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	8
110.83.80.161	China	147.237.77.226	www.chamatz.aka.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.233	atal.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.170	maarachot.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.234	halag.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.176	matpash.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
188.214.249.145	Romania	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
66.135.63.82	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
195.234.228.90	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
172.245.218.130	United States	147.237.76.42	refuah.idf.il	0543: HTTP: php.cgi Access	Block	1
45.32.83.228		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-25-2016-08:04:09 to 01-25-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.135.63.82	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
217.194.206.108	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
80.246.138.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.167	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.161.40.120	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
195.234.228.90	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	1
176.13.12.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.105.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.190.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-25-2016-08:04:09 to 01-25-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.174.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
80.246.133.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	143
66.249.81.163	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	62
37.26.149.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
209.88.198.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
37.26.149.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
40.77.167.27	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
8.37.237.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.52.22.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
95.199.8.43	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.156.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
95.199.15.122	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.22.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.22.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
66.249.81.171	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
2.52.22.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.22.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
110.83.80.161	China	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.140.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.93.161	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
2.54.143.193	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.31.35	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
80.178.157.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.130.77	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.183.31.35	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.54.142.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.127.135.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.61.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.51	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
65.55.210.36	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.32.179.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.160.130	Israel	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
2.54.2.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.116.239.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-25-2016-08:04:09 to 01-25-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
176.13.1.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
176.13.1.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
176.13.4.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
109.253.198.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.253.144.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
109.65.106.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
37.26.149.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.199.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.219.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.179.226.169	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.4.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.131.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.0.27.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
176.13.15.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.40.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
110.83.80.161	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 110.83.80.161	Block	3
2.52.130.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
109.253.156.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.156.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
149.88.113.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
110.83.80.161	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 110.83.80.161	Block	2
188.120.148.148	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
110.83.80.161	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 110.83.80.161	Block	2
110.83.80.161	China	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 110.83.80.161	Block	2
2.54.189.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.253.128.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
110.83.80.161	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 110.83.80.161	Block	2
2.52.160.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.128.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.144.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/3382.jpg	Block	1
185.89.217.235		147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
85.64.40.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/hom×§	Block	1
5.36.174.4	Oman	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
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	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.81.138	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
62.0.27.129	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.0.27.129	Block	1
176.13.15.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.142	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
80.246.137.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-25-2016-08:04:09 to 01-25-2016-09:04:09