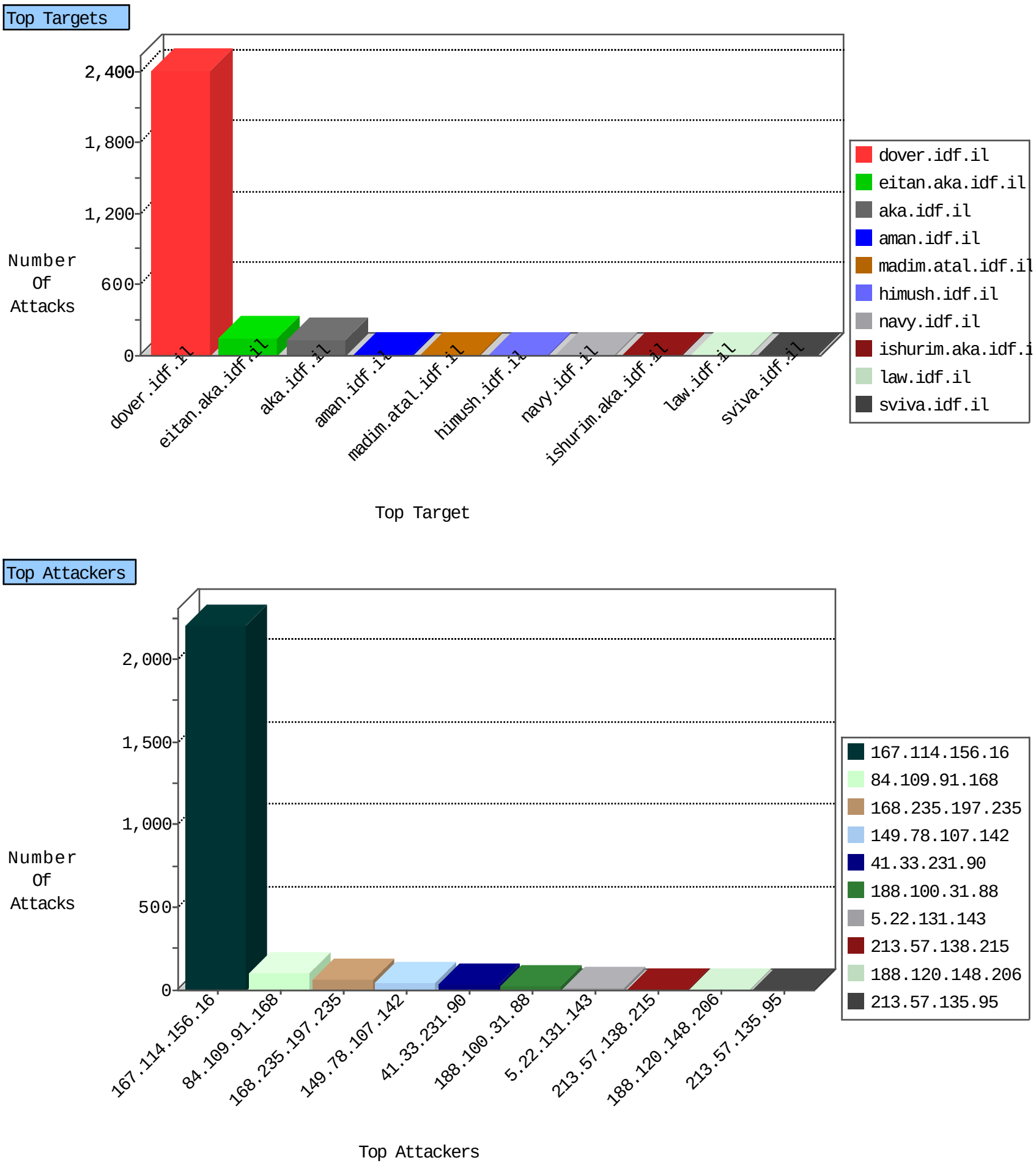
12-06-2015-00:04:02 to 12-06-2015-01:04:02

IDF Under Attack Daily Report



12-06-2015-00:04:02 to 12-06-2015-01:04:02

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	3465
109.64.113.250	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
168.235.197.235	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1

12-06-2015-00:04:02 to 12-06-2015-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-06-2015-00:04:02 to 12-06-2015-01:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
123.56.147.116	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
123.56.147.116	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.170	Canada	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.16	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.16	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
123.56.147.116	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
123.56.147.116	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.155	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.170	Canada	maarachot.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.16	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
123.56.147.116	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1

12-06-2015-00:04:02 to 12-06-2015-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.235	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.109.91.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
188.100.31.88	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
5.22.131.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.120.148.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.148.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.44.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.3.146.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.107.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.127.15.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.0.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
94.230.86.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.179.219.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.218.134.134	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
63.143.207.236	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.57.135.95	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.231.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.135.95	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.68.74.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.154.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.35.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.6		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.222.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.168.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.120.49.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.73.156	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
188.120.148.176	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.138.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.94.140.132	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.90	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.178.218.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
213.57.138.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.120.34.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.133	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.34.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
113.240.250.155	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	2
213.57.138.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.228.35.164	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
2.54.155.89	Israel	147.237.76.86	navy.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.120.49.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

12-06-2015-00:04:02 to 12-06-2015-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.91.168	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
149.78.107.142	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.107.142	Block	33
94.159.166.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
177.12.172.102	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 177.12.172.102	Block	3
78.154.170.6	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	3
2.54.7.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.44.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.129.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
109.64.109.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.219.92.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
37.26.147.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-20704-he/dover.aspx	Block	1
114.98.232.198	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1281-ar/cogat.aspx/trackback/	Block	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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/robots.txt	Block	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
162.209.101.250	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.66.29	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
40.77.167.82	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/giyus/general.aspx	Block	1
87.68.148.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
178.154.243.96	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
122.139.81.49	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
46.120.140.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14077458 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
212.76.107.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.223.122.11	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/1	Block	1
175.184.161.178	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.67.169.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.105.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
149.78.107.142	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/resources/styles/general.css	Block	1
176.12.144.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.160.237.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.200.70	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	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-en/idfgdover.aspx	Block	1
176.13.4.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.154.222	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.69.250	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/1133-22461-he/dover.aspx.	Block	1
80.178.157.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-06-2015-00:04:02 to 12-06-2015-01:04:02