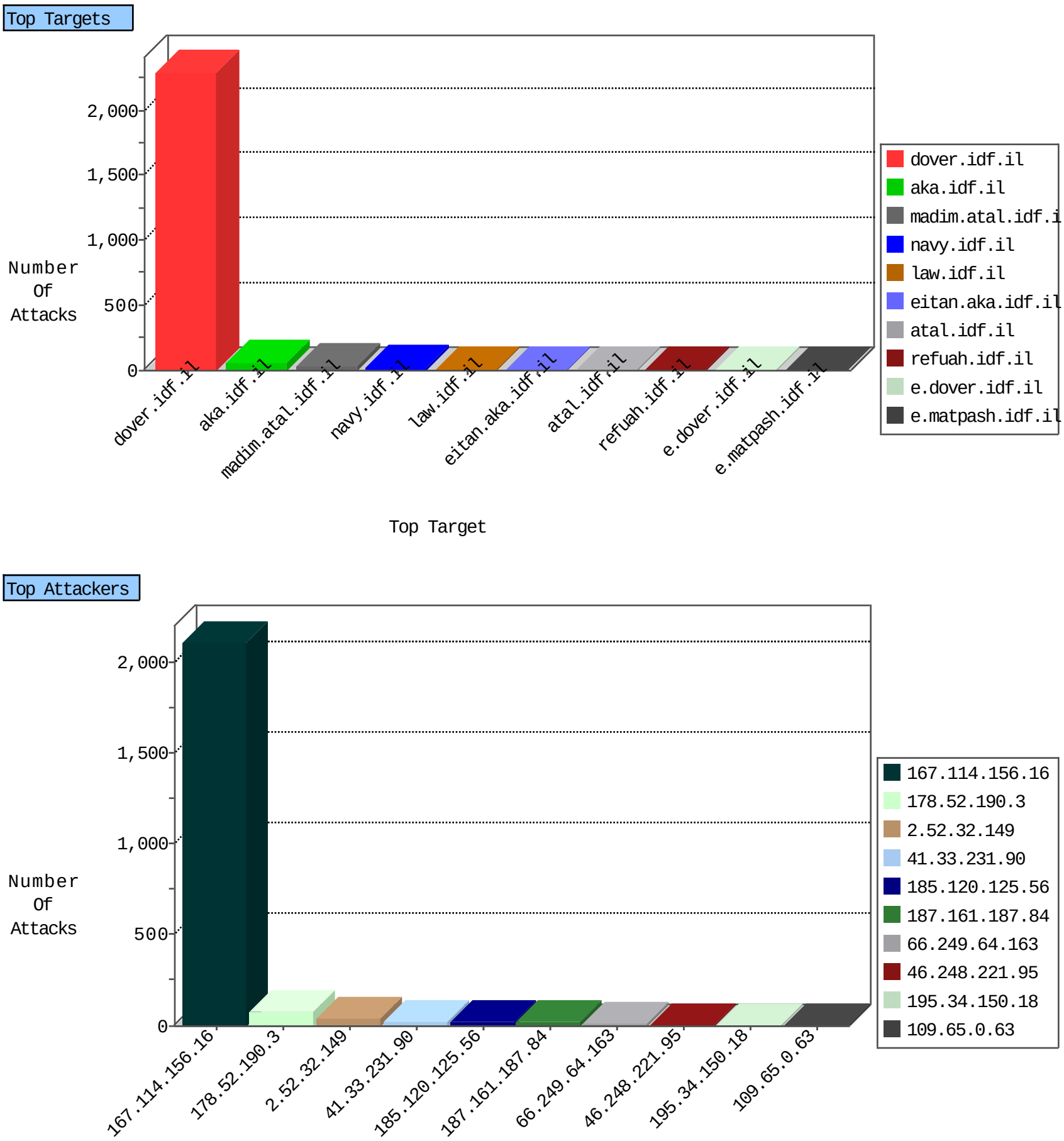
01-13-2016-02:04:06 to 01-13-2016-03:04:06

IDF Under Attack Daily Report



01-13-2016-02:04:06 to 01-13-2016-03:04:06

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	3198
63.141.227.98	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
123.180.15.222	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

01-13-2016-02:04:06 to 01-13-2016-03:04:06

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	2
184.168.193.34	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
67.55.90.132	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.37	France	147.237.76.31	nakchal.idf.i	C228: HTTP: AhrefBot crawler	Block	1
68.48.156.101	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
104.45.31.87	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-13-2016-02:04:06 to 01-13-2016-03:04:06

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.45.31.87	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	3
184.168.193.34	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
68.48.156.101	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
187.161.187.84	147.237.77.205	Mexico	prisha.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
168.62.238.153	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.6.220	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
124.65.231.114	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
201.173.183.106	147.237.72.217	Mexico	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
124.65.231.114	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
124.65.231.114	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.61.20.81	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.151.12.168	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
109.235.254.181	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
201.173.183.106	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-13-2016-02:04:06 to 01-13-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.52.190.3	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
178.52.190.3	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
2.52.32.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.248.221.95	Jordan	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.32.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.52.32.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.32.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
187.161.187.84	Mexico	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
66.249.64.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
187.161.187.84	Mexico	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
187.161.187.84	Mexico	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
190.249.137.122	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
187.161.187.84	Mexico	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.2.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.181.9.247	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
109.65.0.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
66.249.64.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.65.0.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
207.46.13.99	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.88.226.249	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
131.253.24.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
75.186.33.162	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.158	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.1.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
96.255.204.246	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.67.1.25	United States	147.237.0.33	idf.il	drop		drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
131.253.36.206	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.3.147.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.142.68.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.184	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.65.0.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.67.1.25	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.68.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.125.56		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.32.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	2
37.26.147.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	2
157.55.39.152	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	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
8.37.71.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1398-en/dover.aspx?pagenum=2&lang=en&sortdir=asc&usg=alkjrhjtxyfincjw7hwpexi2wp8w2j4ryq	Block	1
187.161.187.84	Mexico	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	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
178.52.190.3	Syrian Arab Republic	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
109.65.0.63	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	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
187.161.187.84	Mexico	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.28.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
178.52.190.3	Syrian Arab Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
114.97.202.91	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/925-he/cogat.aspx/trackback/	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
217.132.157.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.161.187.84	Mexico	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
92.98.29.241	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
141.212.122.145	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	1
157.55.39.109	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	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
8.37.70.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1398-en/dover.aspx&usg=alkjrhgwoznlri8xvcaza42llwljexfthg	Block	1
187.161.187.84	Mexico	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1

01-13-2016-02:04:06 to 01-13-2016-03:04:06