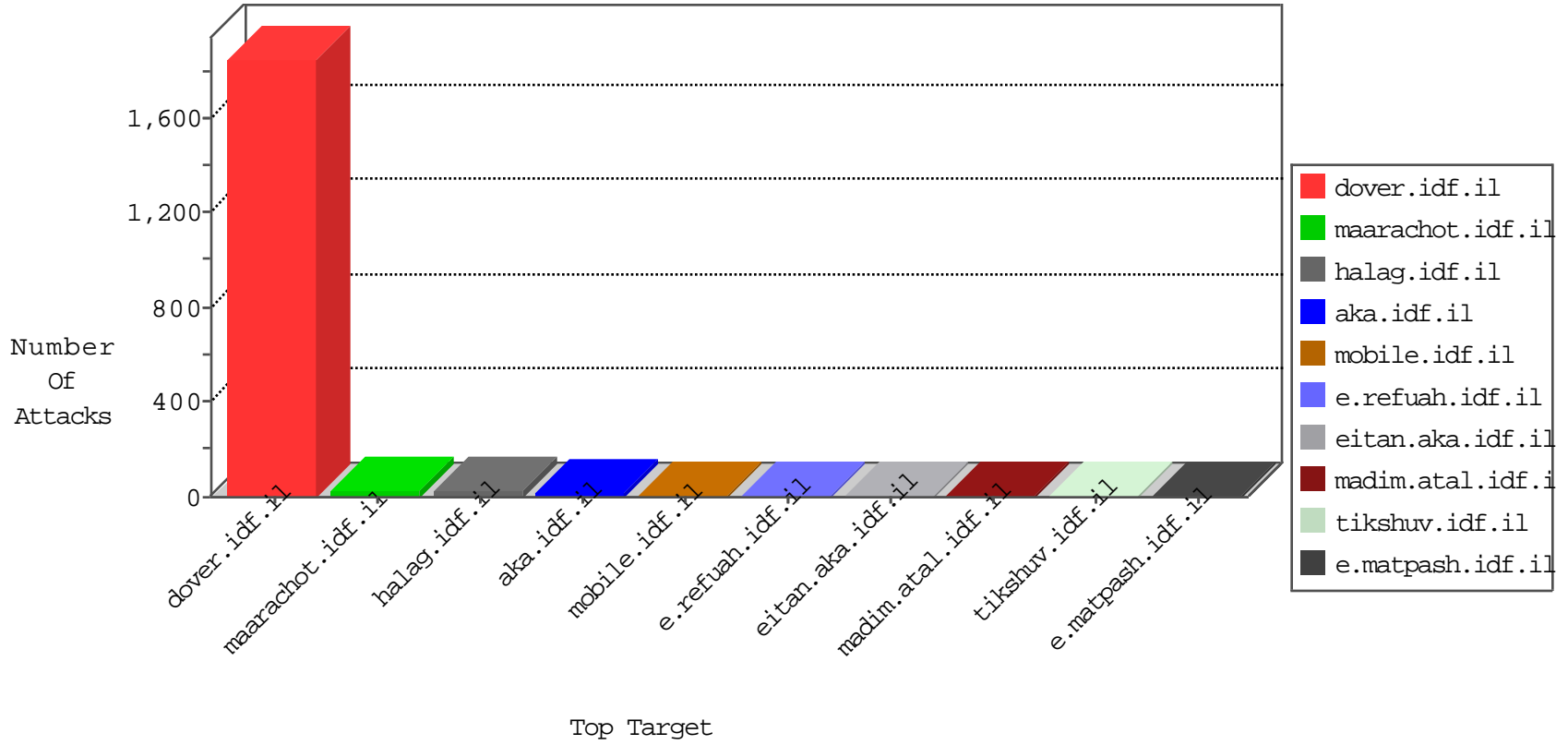


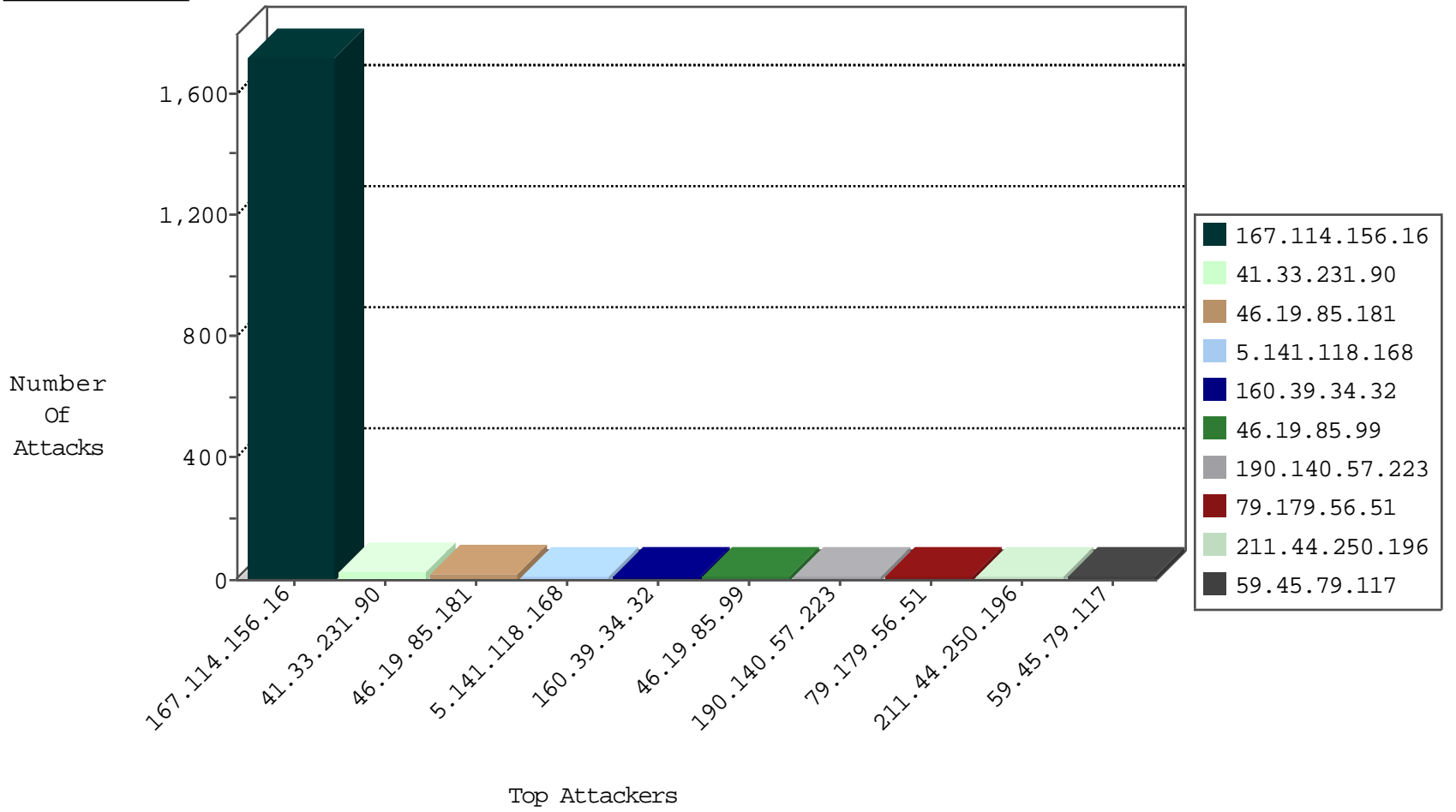
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3260
208.67.1.60	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
46.166.188.68	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-03-2016-04:04:00 to 01-03-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.58.86.14	United States	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1

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
211.44.250.196	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.148	Korea, Republic of	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
120.214.107.170	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.141.118.168	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
118.69.191.166	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
211.44.250.196	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.176	Korea, Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
211.44.250.196	147.237.76.147	Korea, Republic of	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.56.204.89	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.141.118.168	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
118.69.191.166	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
211.44.250.196	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
5.141.118.168	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
160.39.34.32	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
190.140.57.223	Panama	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.179.56.51	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
46.19.85.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.181	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
168.235.196.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.178.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.25.53	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.183.189.131	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
185.100.86.86		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.183.179.194	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
109.201.152.5	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.124	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
184.105.139.75	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.126	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.25.193.20	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
216.218.206.74	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.130.5.224		147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
184.105.139.83	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.36.236	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
153.183.9.157	Japan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.239	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
51.255.202.66	United Kingdom	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
176.10.99.207	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
216.218.206.102	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2
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	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
109.253.222.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.137.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
64.19.78.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
69.197.169.202	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
184.105.139.68	United States	147.237.0.16	ny-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
149.202.98.160	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
78.79.28.241	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/netunim.stm.	Block	1
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	1
109.67.212.205	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
84.111.124.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.237	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
136.243.48.82	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
69.197.169.202	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1