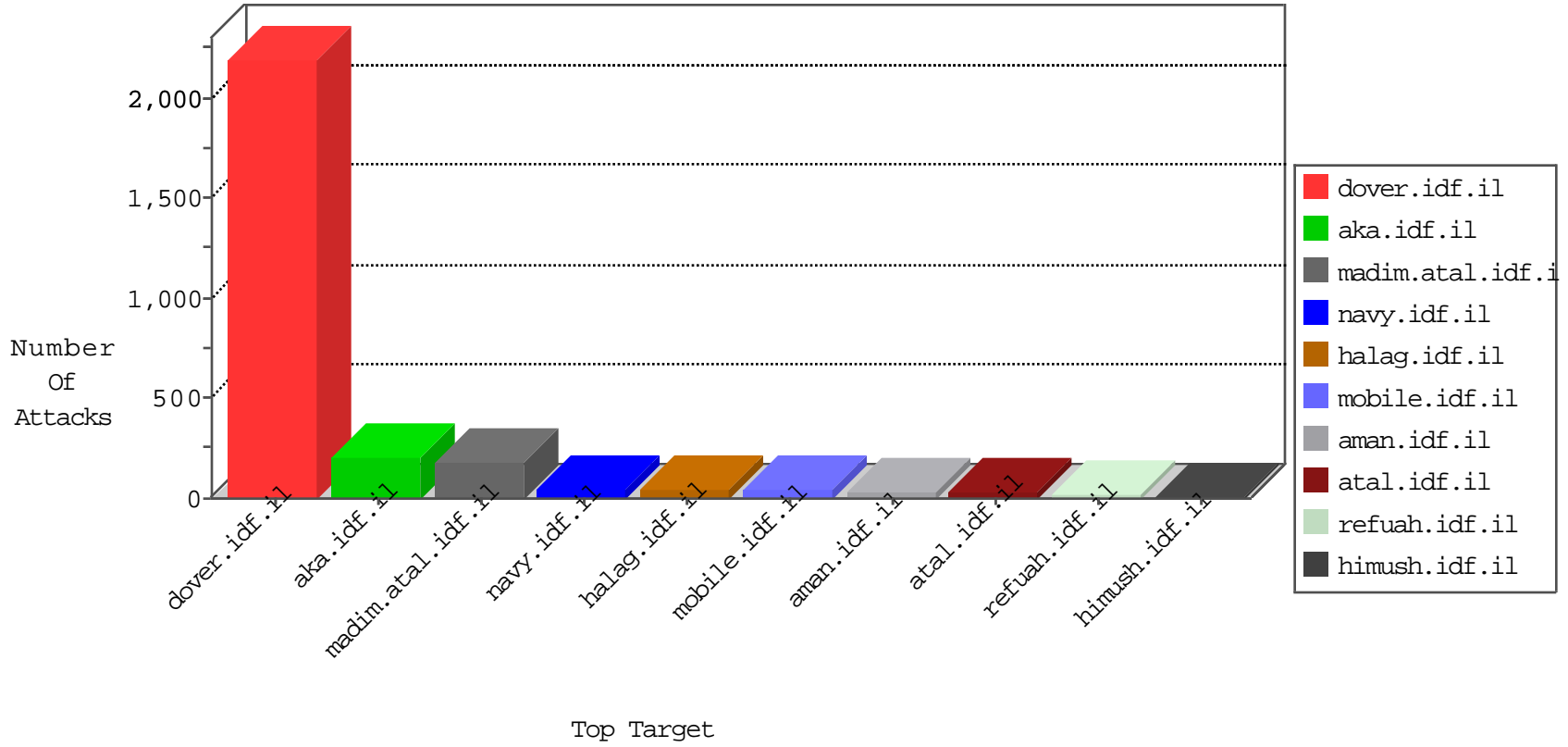


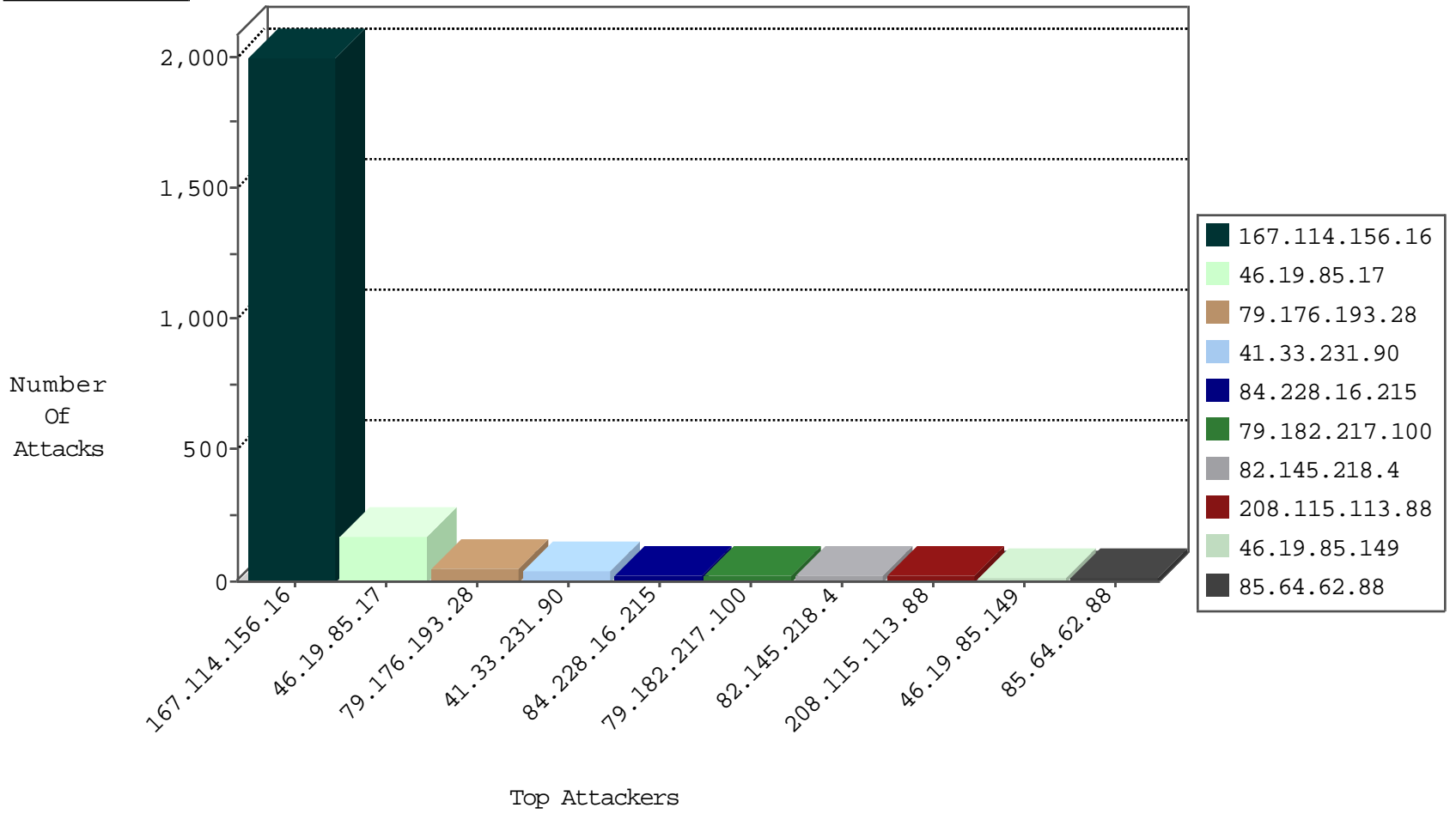
IDF Under Attack Daily Report



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	3223
42.3.193.208	Hong Kong	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2

12-26-2015-16:04:00 to 12-26-2015-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.246.183.211	147.237.0.33	Indonesia	idf.il	ET SCAN NMAP -sS window 1024	1
123.143.79.107	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
123.143.79.107	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.143.79.107	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.177	Netherlands	noore.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.49.211	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
31.19.116.8	147.237.76.86	Germany	navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.148	China	gcqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.246.183.211	147.237.0.33	Indonesia	idf.il	ET SCAN NMAP -sS window 3072	1
123.143.79.107	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
123.143.79.107	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
123.143.79.107	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
219.79.98.139	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.245.15.126	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.193.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
82.145.218.4	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
84.228.16.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.182.217.100	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
85.64.62.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.246.139.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.177.158.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.153.29	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.94.57.139	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.217.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.182.126.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.181.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.34.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	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
89.139.146.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.32.179.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.3.144.57	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
185.32.179.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	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
5.22.134.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.193.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.177.191.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.3.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
23.254.243.147	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.128	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.16.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.132.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.153.29	Israel	147.237.76.30	himush.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.10.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.137.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.184	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.178.36.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	17
168.235.197.199	United States	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in Session from 168.235.197.199	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
84.228.16.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.177.222.13	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
93.172.34.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.35.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.222.13	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/1/	Block	3
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
23.254.243.147	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
77.126.61.12	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.13.66	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
185.120.125.45		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.17.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
75.98.175.87	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
79.183.186.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
108.179.251.85	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
87.69.158.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.115	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/1133-22638-he/dover.aspx.	Block	1
5.22.134.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.151.154.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.55.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter 0559c450 in www.aka.idf.il/main/home/default.aspx	None	1
75.98.175.87	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
46.121.140.73	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
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.109.240.130	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.109.240.130	Block	1
37.26.146.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
198.58.103.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
79.177.222.13	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.177.222.13	Block	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
109.65.161.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/global.js	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
5.28.181.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
194.150.113.90	Denmark	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.182.209.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
75.98.175.87	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1
46.166.190.161	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.142.68.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	1
185.36.100.145	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1