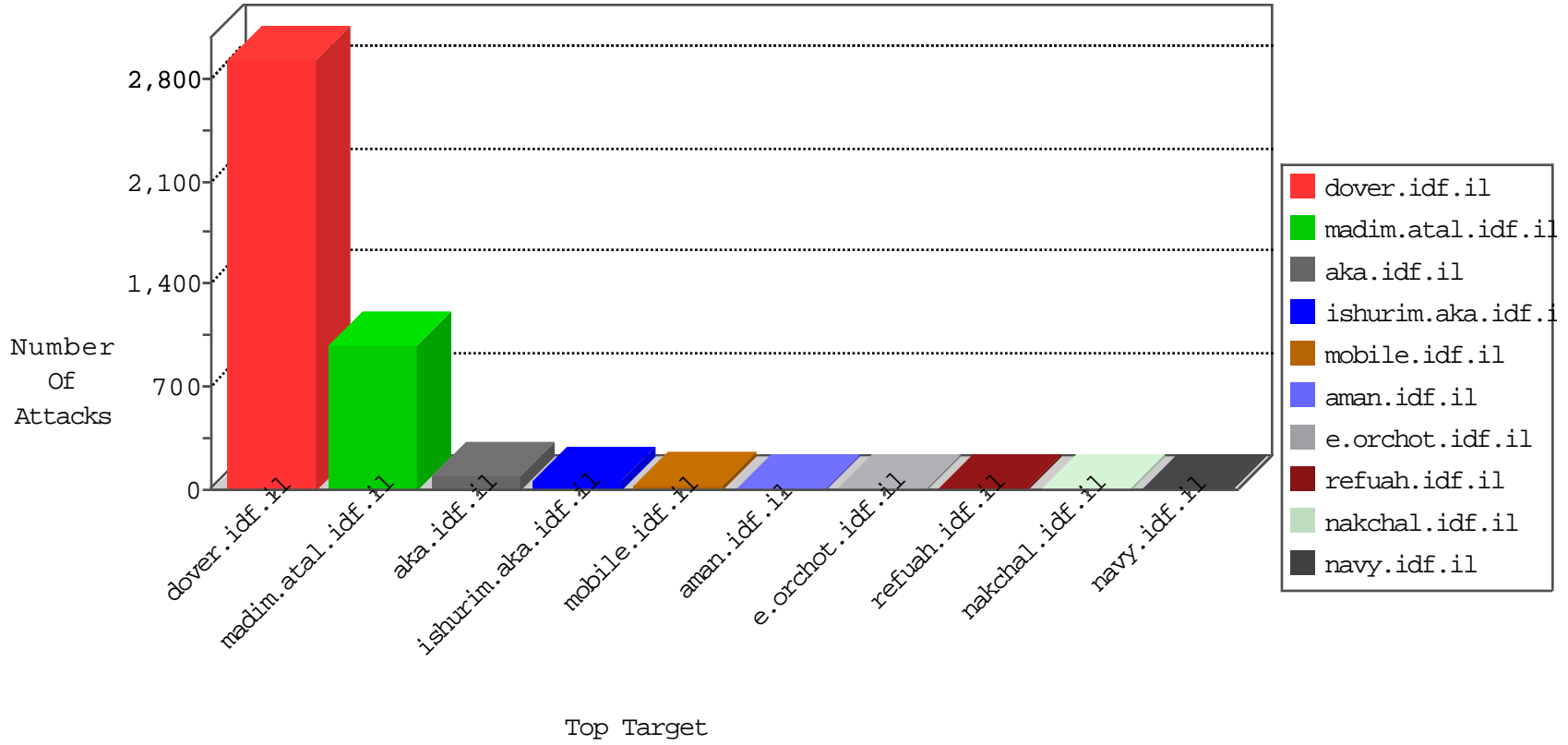


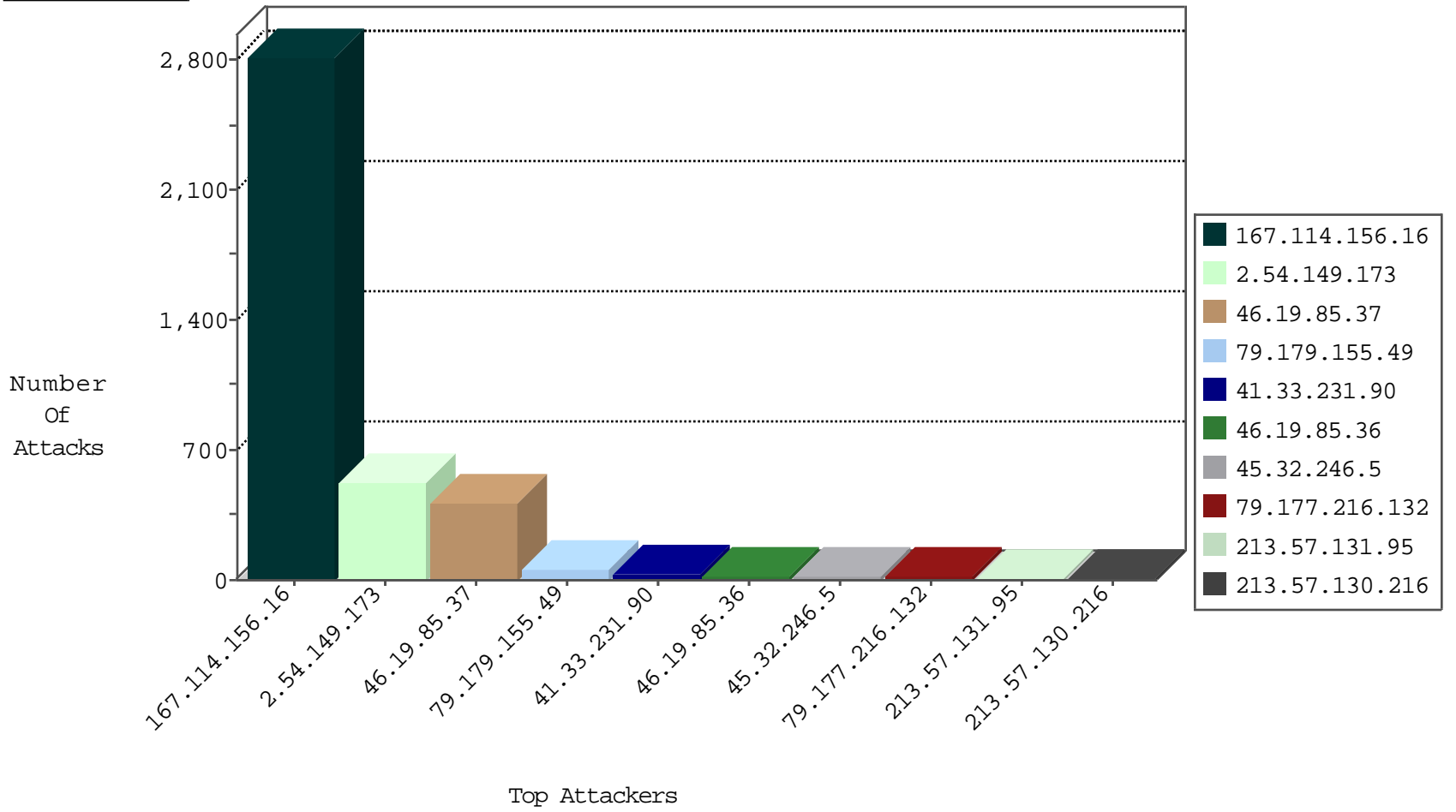
IDF Under Attack Daily Report



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	3443
45.32.246.5		147.237.8.24	e.lifestyle.idf.il	Invalid TCP Flags	drop	4
45.32.246.5		147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	3
71.6.216.56	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.50.45	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.8	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1
167.88.7.250	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1

12-09-2015-07:04:07 to 12-09-2015-08:04:07

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
91.201.236.113	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.177.106.170	147.237.8.46	India	e.chinuch.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.246.5	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.246.5	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
31.210.187.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.76.196	Ukraine	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.246.5	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.246.5	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -f -sS	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	36
79.177.216.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
213.57.131.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.167.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.106.94.2		147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
37.26.146.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.130.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.130.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
45.32.246.5		147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	4
37.46.39.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.134.127.3	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.27.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.142.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.91.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.176.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.131.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.229.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.125.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.39.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.134.127.3	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.190.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.217	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
198.20.87.98	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
207.46.13.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.130.190.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
65.55.210.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.67.103.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
85.130.190.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.23	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
180.97.106.161	China	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.57.140.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.28.159.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.116.127.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.149.173	Block	279
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.149.173	Block	75
79.179.155.49	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	12
46.120.216.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.142.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.217.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
80.246.139.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.139.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.153.105.109	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	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
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
79.182.57.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.57.174	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
79.180.217.196	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.217.196	Block	2
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
72.229.130.220	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.225.111.98	United States	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.mag.idf.il/163-7129-en/patzar.aspx	Block	1
37.26.148.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.226.39	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.97.116.171	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 209.88.198.1	Block	1
72.229.130.220	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.64.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1111-7650-he/nakhal.aspx	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.180.217.196	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
2.54.62.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.241.226.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
66.249.66.48	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.141.143	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
199.30.24.139	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
109.67.103.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71840-he/maarachot.aspx	Block	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
46.166.186.206	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.168.125.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainqsachar	Block	1
93.172.141.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/defaulthttps://www.facebook.com/video.php	Block	1