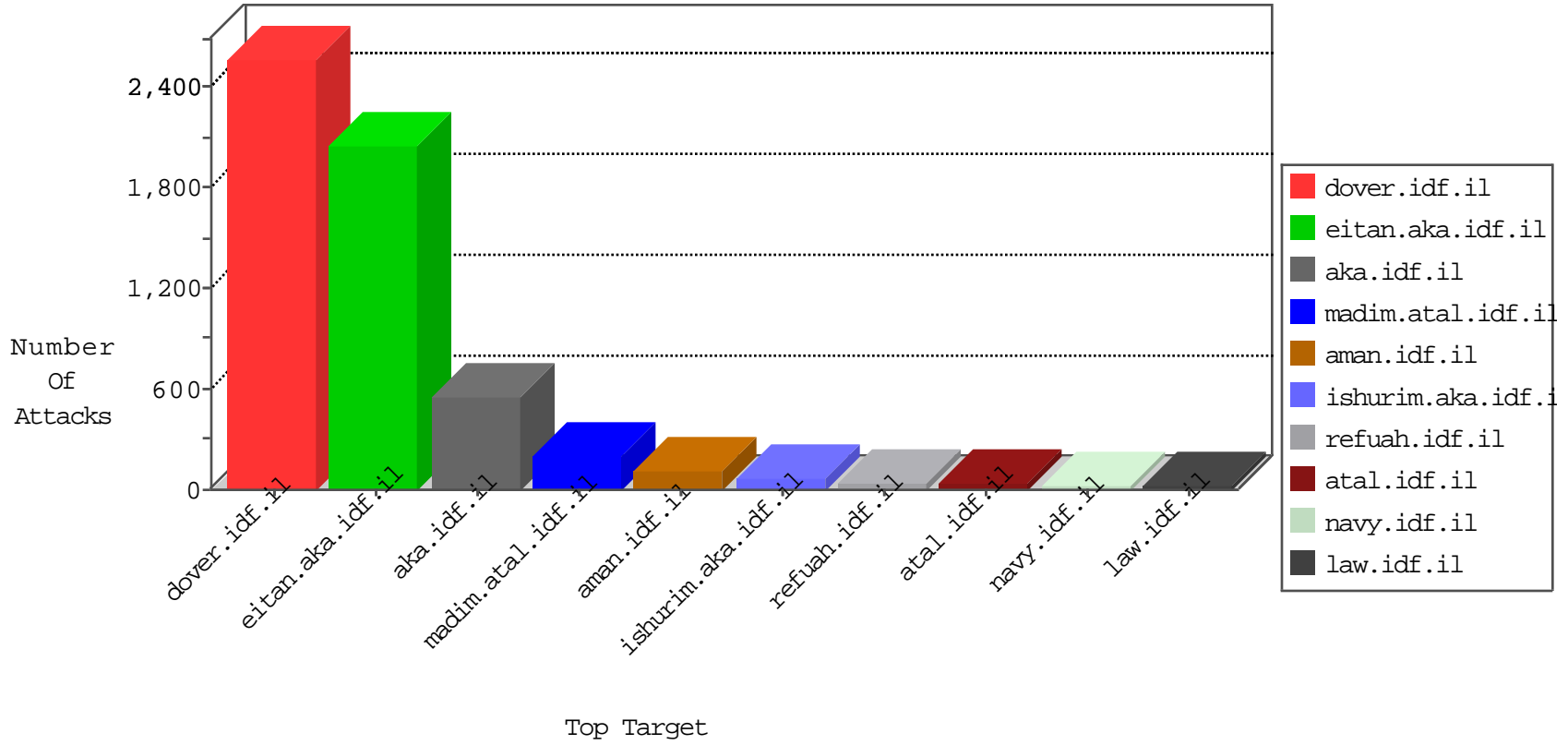


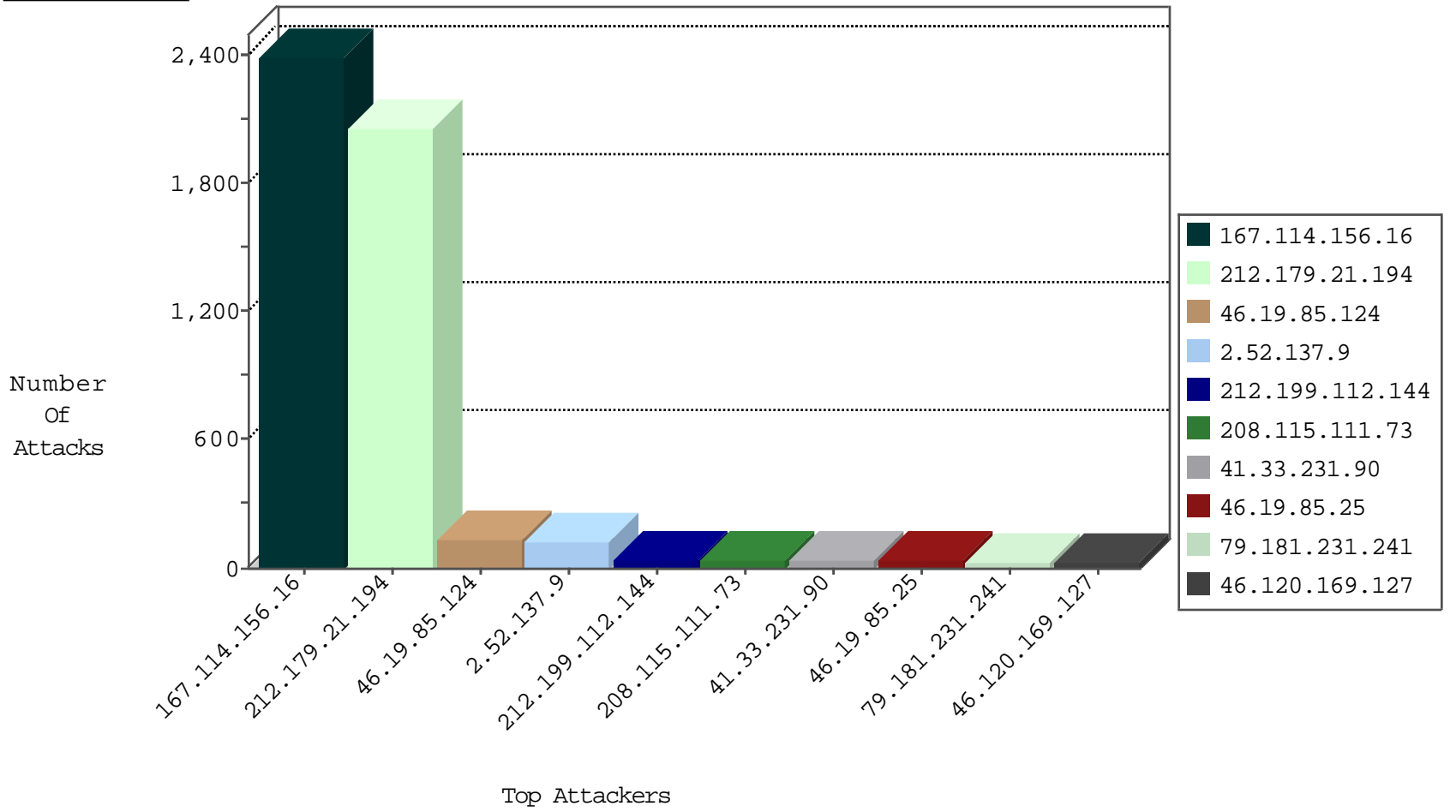
IDF Under Attack Daily Report



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	3635
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
116.224.195.151	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
219.151.9.44	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
167.88.12.197	United States	147.237.77.74	law.idf.il	block-sp-trafl	drop	1
71.6.158.166	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.238	United States	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
1.36.208.29	Hong Kong	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
167.88.12.210	United States	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
167.88.7.254	United States	147.237.76.30	himush.idf.il	block-sp-trafl	drop	1
31.205.98.190	United Kingdom	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
121.3.42.72	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
167.88.10.197	United States	147.237.77.19	law-forum.idf.il	block-sp-trafl	drop	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.174.254.199	United Kingdom	147.237.77.233	atal.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.112	Italy	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
162.210.196.100	United States	147.237.77.216	doover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.98	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.137.9	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	68
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
46.120.128.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.26.137.112	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.72.166	Singapore	aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.67.211.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.160.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.164.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.174.254.199	147.237.77.233	United Kingdom	atal.idf.il	SERVER-WEBAPP admin.php access	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
120.26.137.112	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.72.166	Singapore	aka.idf.il	ET SCAN NMAP -sS window 3072	1
84.228.27.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.52.137.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.181.231.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
213.57.134.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
109.201.152.7	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	11
46.19.85.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.69.10.143	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.116.114.226	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.29.32	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.250.145.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.179.31.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.141.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.90.211	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.137.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
60.49.39.32	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.137.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
95.133.94.113	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.52.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.137.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
95.133.94.113	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.176	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.32.179.185	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.117.6.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.3.146.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.228.146.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.92	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
123.2.172.246	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.67.211.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.140.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
109.67.211.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.35.26.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.29.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.160.239.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	1890
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.124	Block	29
2.54.146.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.120.169.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.169.127	Block	21
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	19
84.108.214.206	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	7
84.108.214.206	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.108.214.206	Block	6
37.26.146.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.6.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.21.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.174.254.199	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 217.174.254.199	Block	3
37.26.146.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.38.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.49.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.174.254.199	United Kingdom	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	2
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
79.179.31.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.169.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.137.245	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.151.53.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewjnh7ya88njahxjvrokhdxdtsqfggmmaa&usg=afqjcneeywysowwococycbntx0qxav9lkw	Block	2
80.246.139.116	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.119	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
212.179.21.194	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
37.26.147.166	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
113.176.180.115	Vietnam	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
94.159.170.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyius/resources/images/home/ajax-loader.gif	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
46.120.169.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.19.85.43	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method gzip, in URL deflate,	Block	1
141.212.122.129	United States	147.237.0.15	kosher-kravi.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
79.182.151.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
23.25.225.221	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.46.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.208.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.153	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.252.88.187	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.238.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.148.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
113.176.180.115	Vietnam	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1