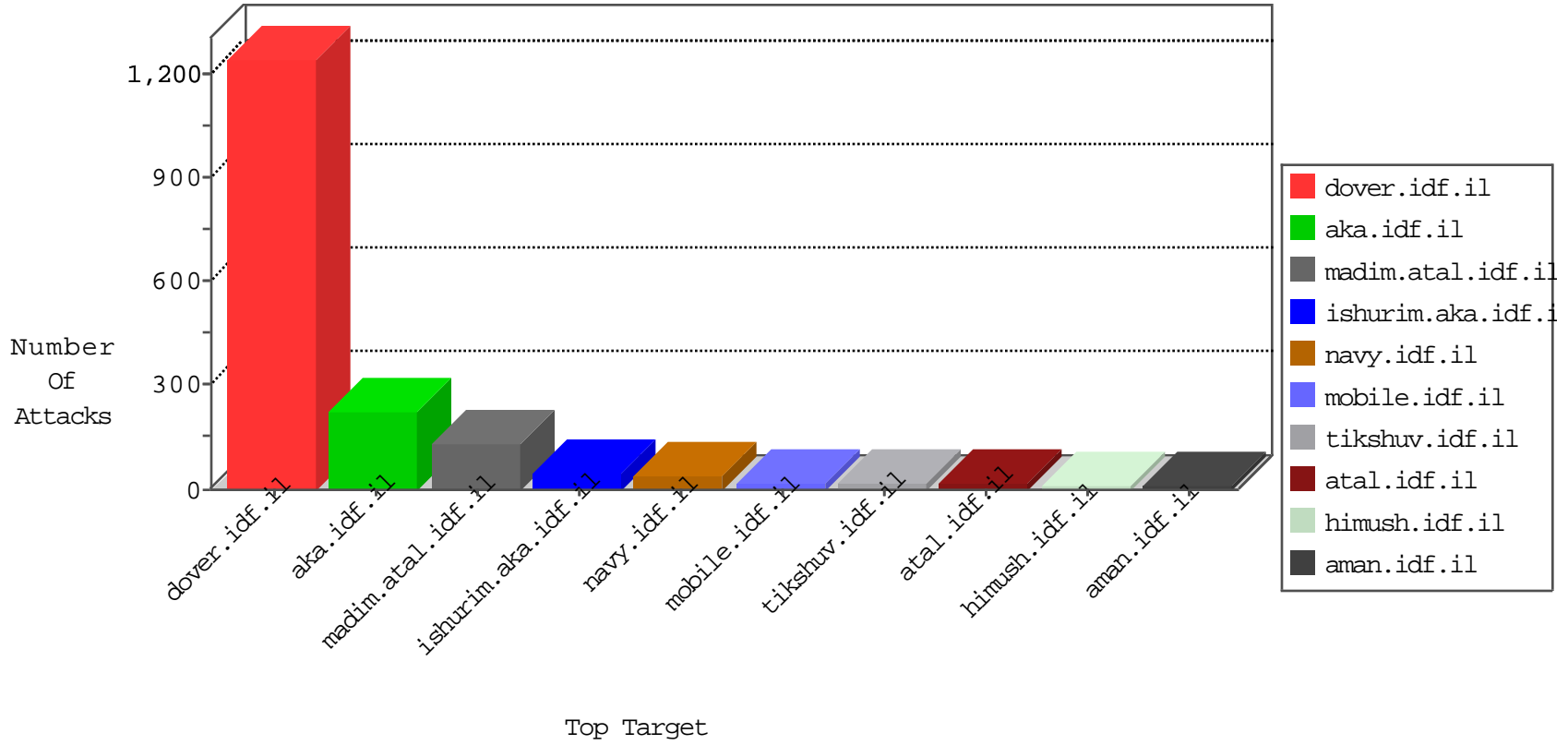


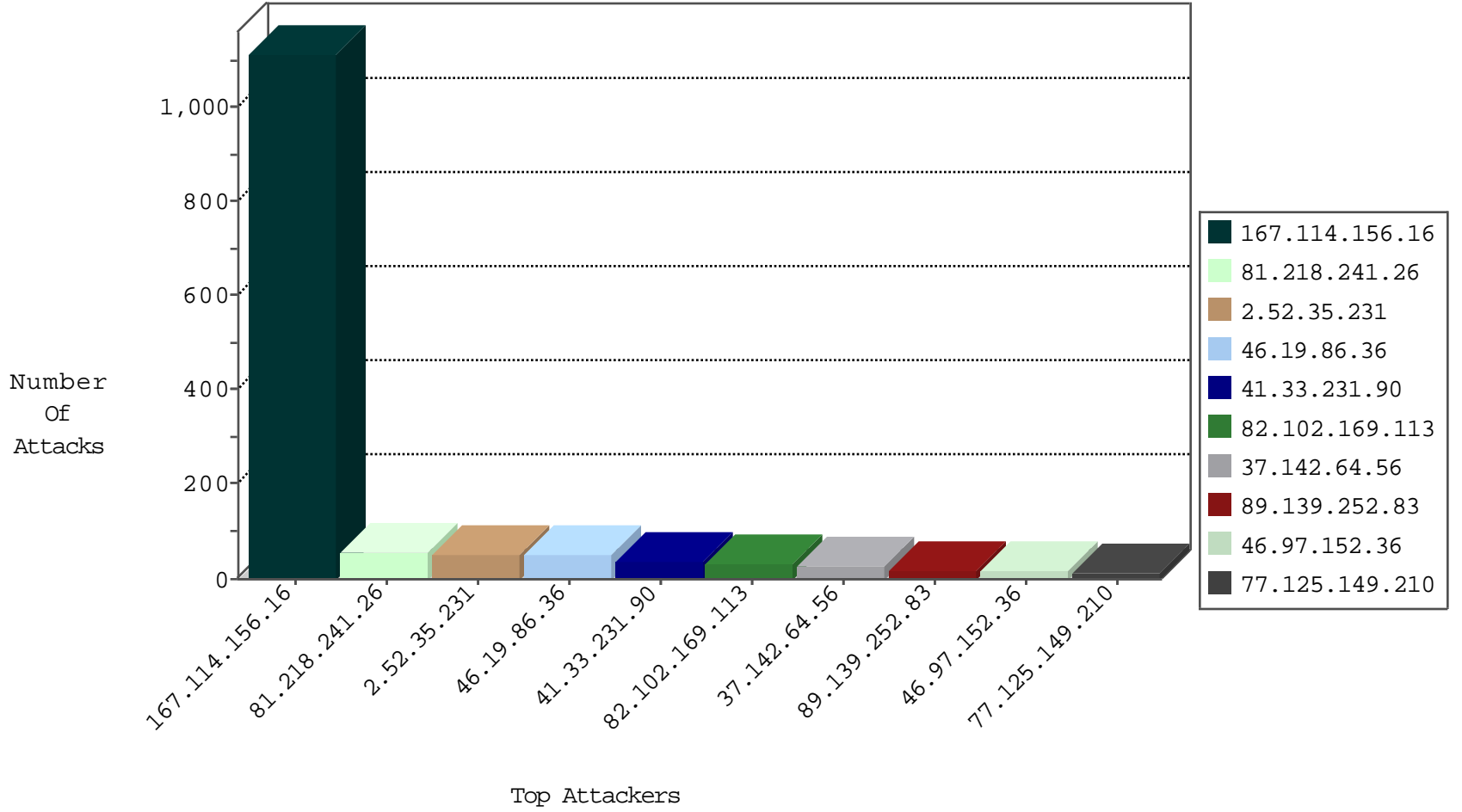
# IDF Under Attack Daily Report



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	3168
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	243
79.181.150.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
65.181.113.88	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
65.181.113.88	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

01-10-2016-07:04:08 to 01-10-2016-08:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDF

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
2.52.35.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.15	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
112.168.26.199	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
106.75.199.201	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.60.252.84	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.203	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.167.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.80.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.15	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
120.198.117.100	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.168.26.199	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
186.116.56.51	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.124.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
76.242.104.129	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.77.179	Russian Federation	e.mazi.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	36
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
37.142.64.56	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
46.97.152.36	Romania	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.142.64.56	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
100.127.210.156		147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
77.125.149.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.20.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
166.142.125.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.184	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.35.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.176.50.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.35.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.50.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.35.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.44.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.35.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.35.231	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
77.125.149.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.148.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.52.35.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.35.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.20.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.35.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.35.231	Israel	147.237.77.216	dover.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
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.35.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.180.64.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.64.185.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.241.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.151.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.188.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.19	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.186.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.218.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.13.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.12.237	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.193.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.113.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.253.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.32.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
89.139.252.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.128.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
93.172.151.172	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.151.172	Block	9
185.32.179.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	3
176.13.20.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.121.79	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.121.92.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	2
109.253.203.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
84.228.78.60	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
2.54.60.137	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
79.182.152.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.111	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/news/	Block	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
106.75.199.201	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.139.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.181.185	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=57272	Block	1
79.176.50.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
182.50.132.37	Singapore	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/xmlrpc.php	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2331.jpg	Block	1
2.54.145.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.1.182	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
79.183.196.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
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	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.54.15.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
79.176.123.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.219.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
37.26.146.234	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	1
80.246.133.183	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.20.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1