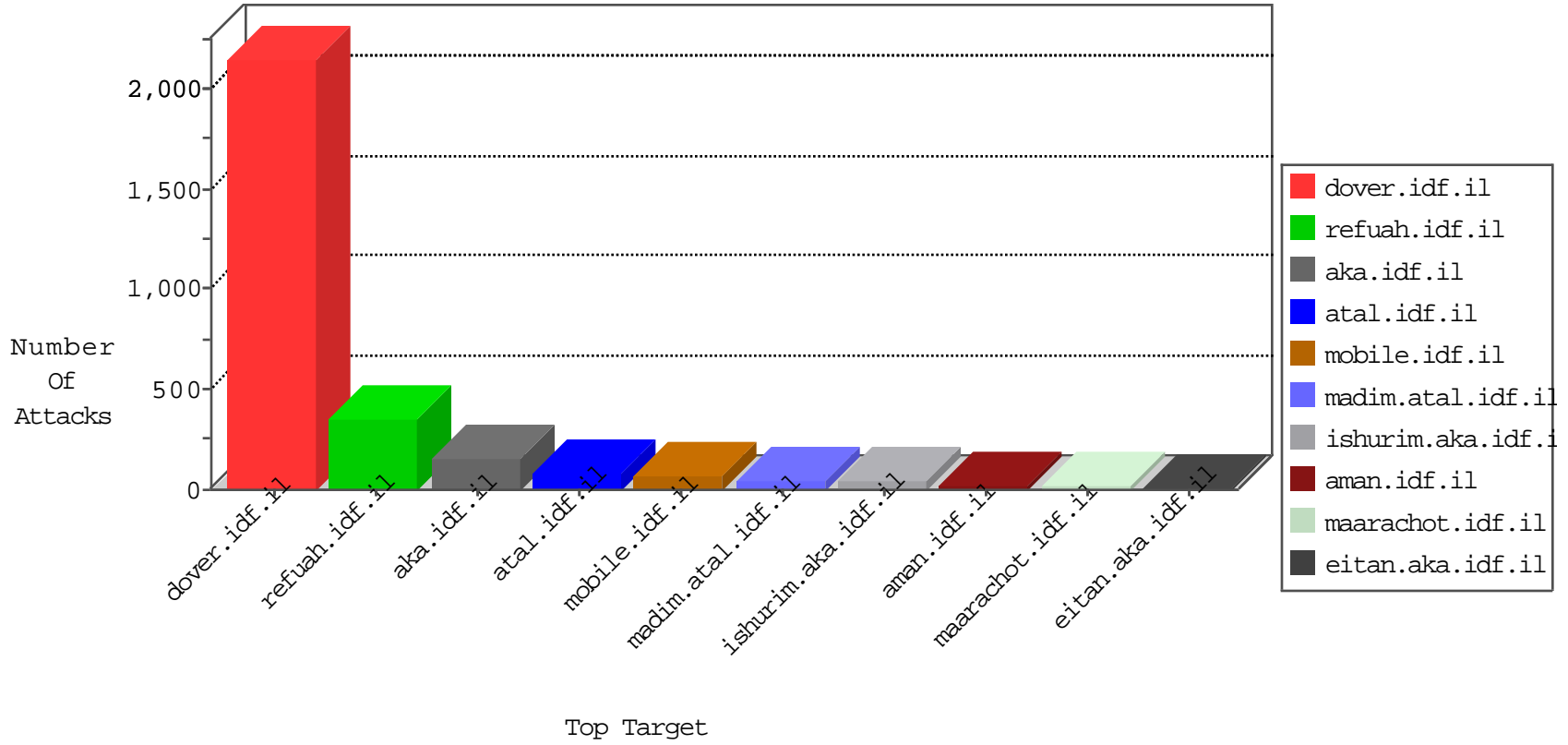


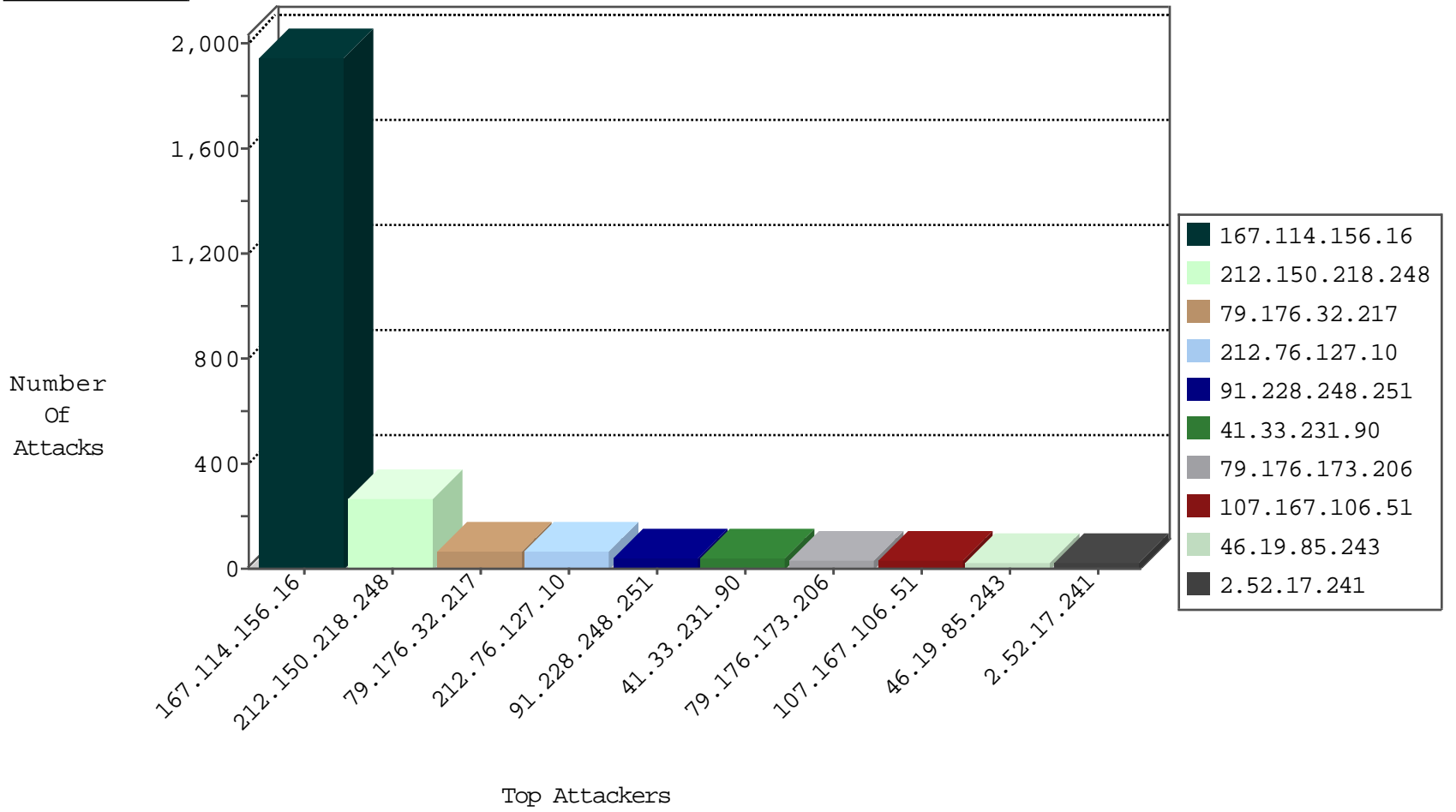
IDF Under Attack Daily Report



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	3469
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
221.118.30.101	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
115.239.248.30	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
204.42.253.2	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
89.248.167.141	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.133	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
107.150.55.213	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
141.212.122.129	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.167.141	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.140	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.77	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
141.212.122.130	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.167.141	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.141	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
115.239.248.30	China	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	1
141.212.122.132	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.167.141	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-09:04:01 to 01-08-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	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
114.236.225.83	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.210.214.89	147.237.0.33	France	idf.il	ET SCAN Potential SSH Scan	1
43.245.183.201	147.237.77.205	Japan	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
43.245.183.201	147.237.77.205	Japan	prisha.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.7	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
1.93.129.5	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
188.53.19.101	147.237.76.34	Saudi Arabia	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
1.93.129.5	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gpcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
167.88.9.227	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
82.102.170.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
43.245.183.201	147.237.77.205	Japan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
1.93.129.5	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.7	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
1.93.129.5	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
188.53.19.101	147.237.76.34	Saudi Arabia	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.33	United States	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
212.150.218.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	268
79.176.32.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.106.51	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
109.64.1.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.56.72.100	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
37.26.146.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.203.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.98.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.157.87	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.67.71.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.18.66	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.2.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.17.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.17.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.141	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
95.35.93.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.17.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
199.30.25.57	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.17.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.17.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
2.52.9.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.168	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.3.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.154.157.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.153.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.199.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.153.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.182.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.188.237	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.69.38	United States	147.237.77.243	mobile.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
109.66.104.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.167.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.157.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.176.173.206	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.173.206	Block	21
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 91.228.248.251	Block	17
79.176.173.206	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	8
85.65.245.0	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	4
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.12.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.3.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.211.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
2.52.189.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.179.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.188.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	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
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.159.123	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
109.64.3.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.36.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.220.156.119	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
91.200.12.106	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113339.pdf#search=	Block	1
37.187.56.81	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
109.253.213.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	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
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58603&docid=71160	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
217.132.56.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.201.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/5/685.pdf	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
91.228.248.251	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1
192.243.55.130	Dominica	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/chanatz/kurs/default.asp	None	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	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
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/englisch	Block	1
80.246.137.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1