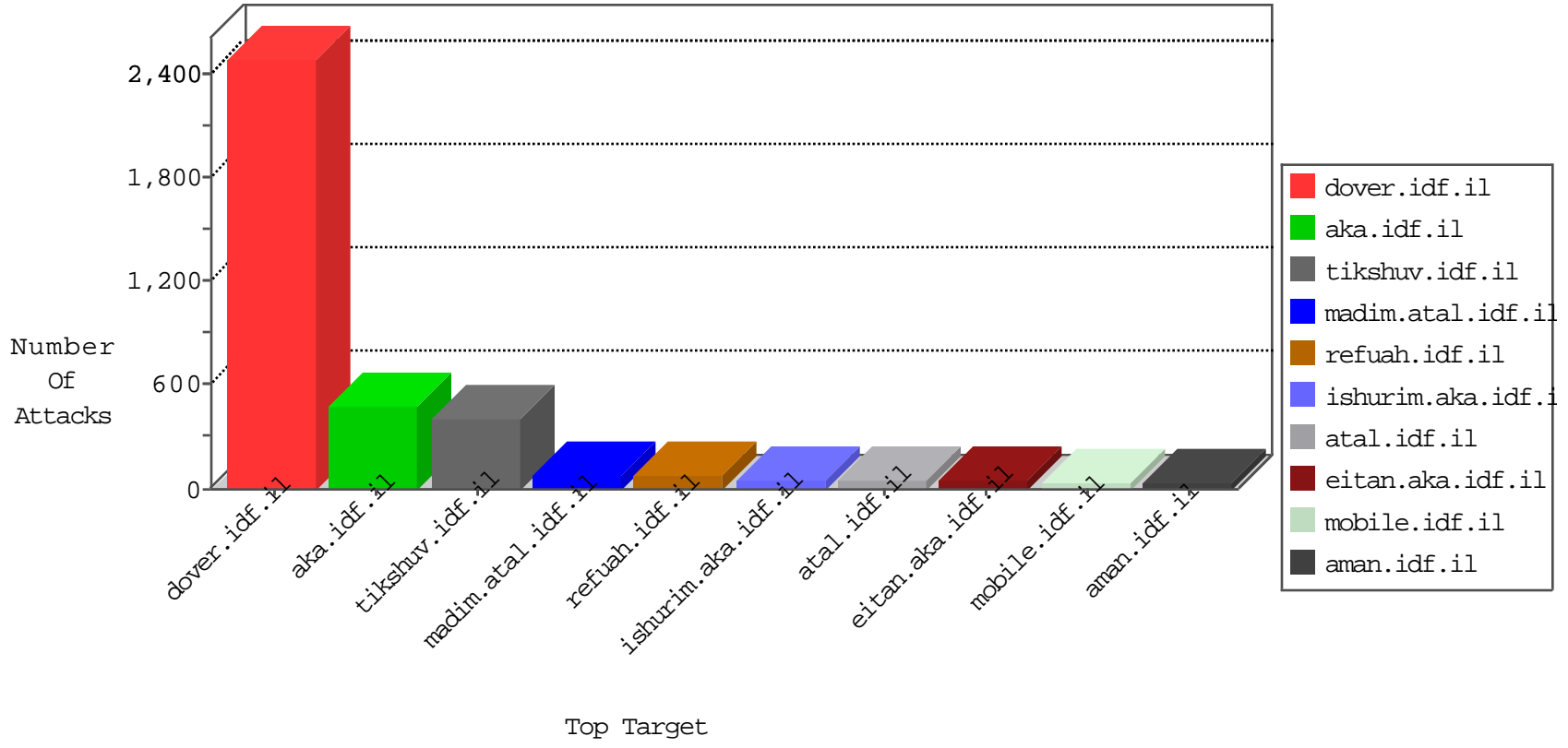


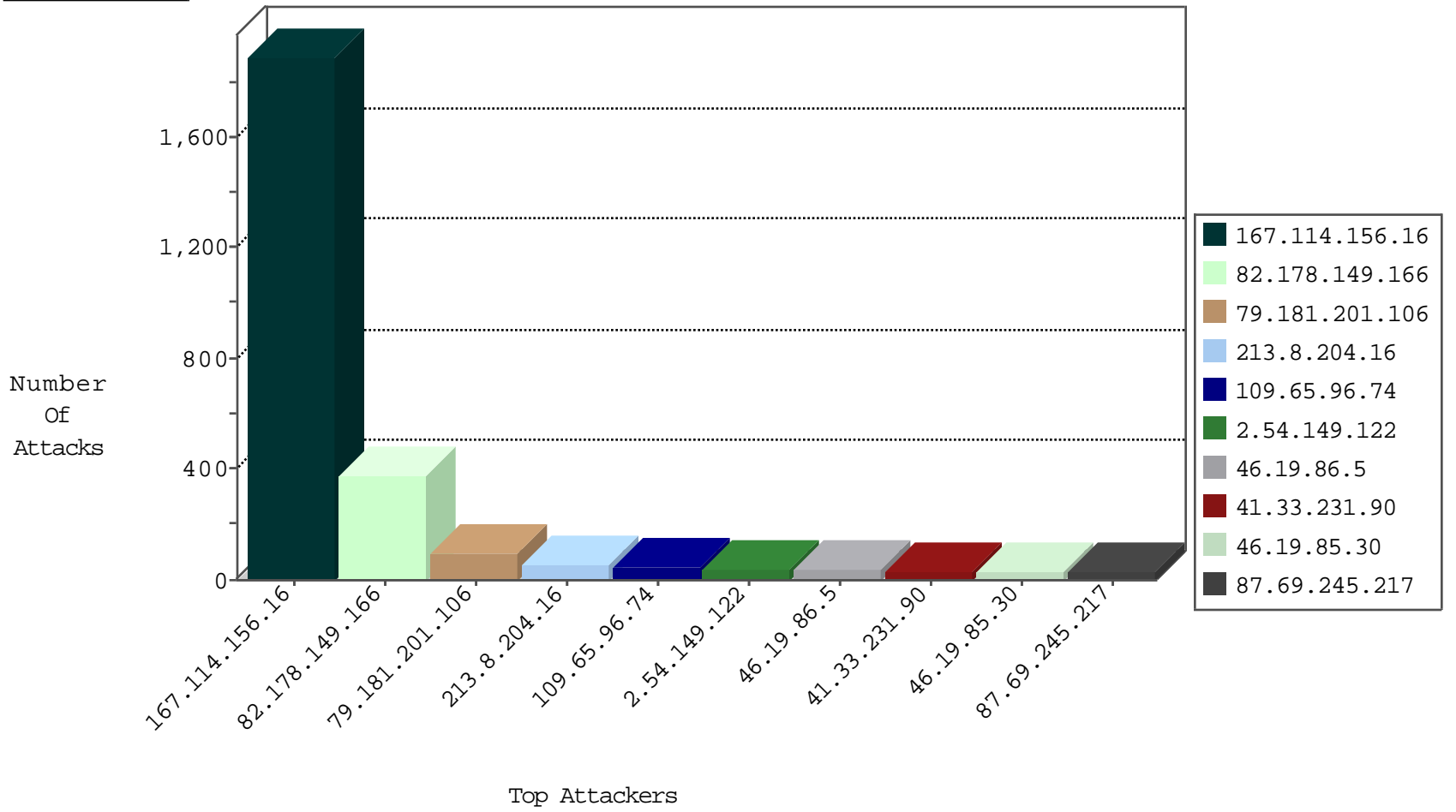
IDF Under Attack Daily Report



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	3098
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	62
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.66.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.178.149.166	Oman	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
128.242.249.12	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.220.182.246	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

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
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	149
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
151.217.97.185	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.175.216	147.237.77.176	Singapore	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.168.213	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.167	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
190.137.67.121	147.237.77.121	Argentina	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.193.2.8	147.237.77.176	France	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.102.254.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.253	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.13.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.169.71.20	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.168.213	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.27.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
73.17.14.46	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.8.45		e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.39.222.253	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.77.235		sviva.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
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop	SAM rule	drop	167
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
109.65.96.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop		drop	29
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
52.89.76.52	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.74.139.99	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.193.24.170	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.68.74.251	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.76.32.115	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
54.65.161.147	Japan	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.69.105.14	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.76.46.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
54.69.147.194	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.69.203.189	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
54.169.210.74	Singapore	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.88.168.51	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.69.248.135	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
77.74.48.226	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
46.19.85.22	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.109.132.138	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
94.230.86.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
128.127.107.123	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
149.78.252.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.69.245.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.69.245.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
87.69.245.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.149.122	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.25.69.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.187.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
14.166.85.187	Vietnam	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.152.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.53.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.187.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.133.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
14.166.85.187	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.145.87	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.187.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.28.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.201.106	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
213.8.204.16	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
2.54.149.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.168.246	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.168.246	Block	23
2.54.145.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
185.120.126.40		147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
2.52.36.114	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
93.172.153.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 93.172.153.78	Block	7
37.26.148.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
5.22.134.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
176.13.6.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.190.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.179.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.248.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
89.139.161.103	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
109.65.105.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.127.107.123	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.142.64.55	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.8.203	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
2.54.10.145	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.221.91	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
84.109.33.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.54	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$ucFaqControl\$txtSearch in www.refua.atal.idf.il/1730-he/refuah.aspx	Block	2
79.180.176.59	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.134.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.16.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.46.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.50.77.124	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.174.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.145.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.144.24	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.149.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.62.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
104.194.26.205	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
79.177.102.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.61.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
87.69.81.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.207	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.130.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.160.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.144.83	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.234.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.195.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.63.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.188.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
180.76.15.152	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.168.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21811-he/idfgdover.asp	Block	1