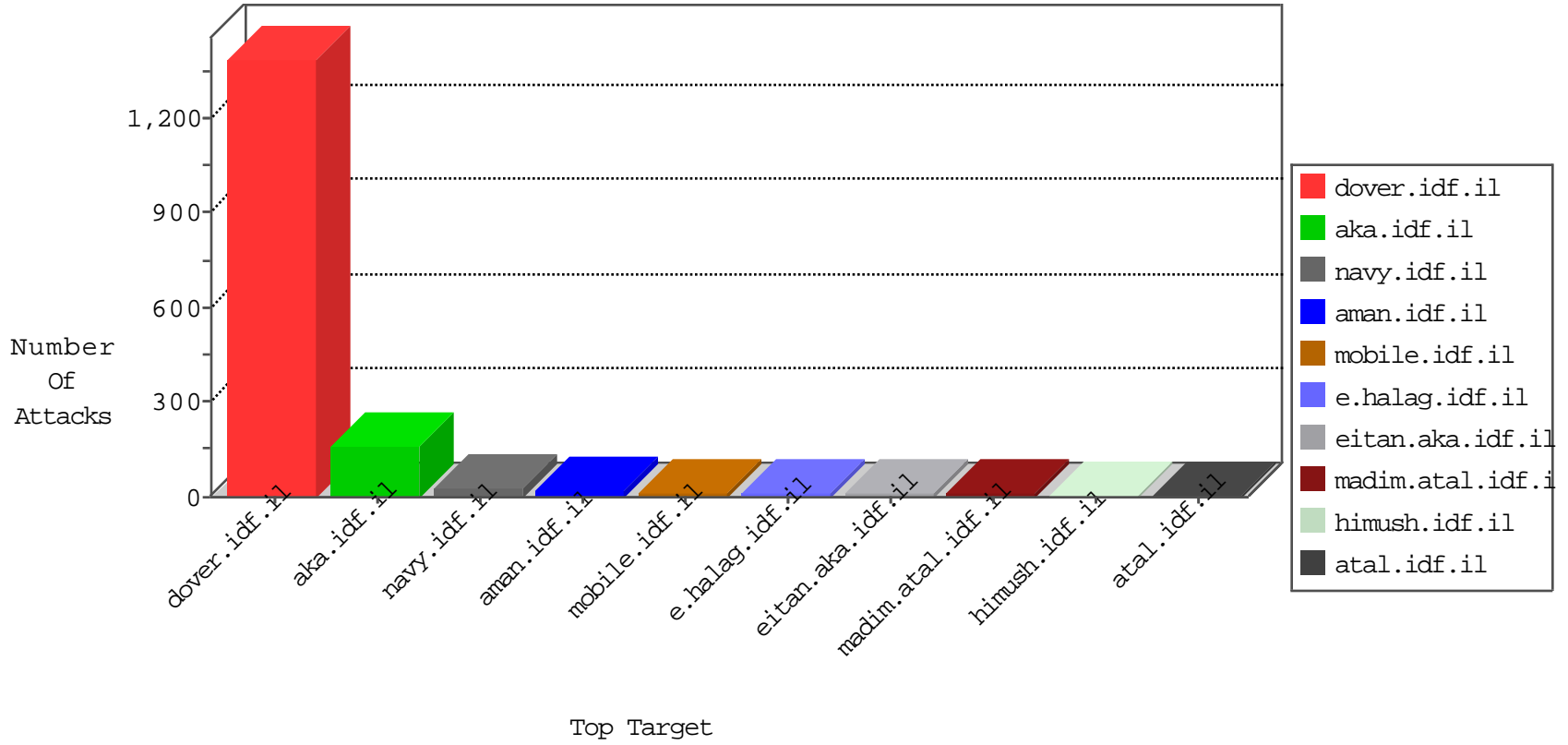


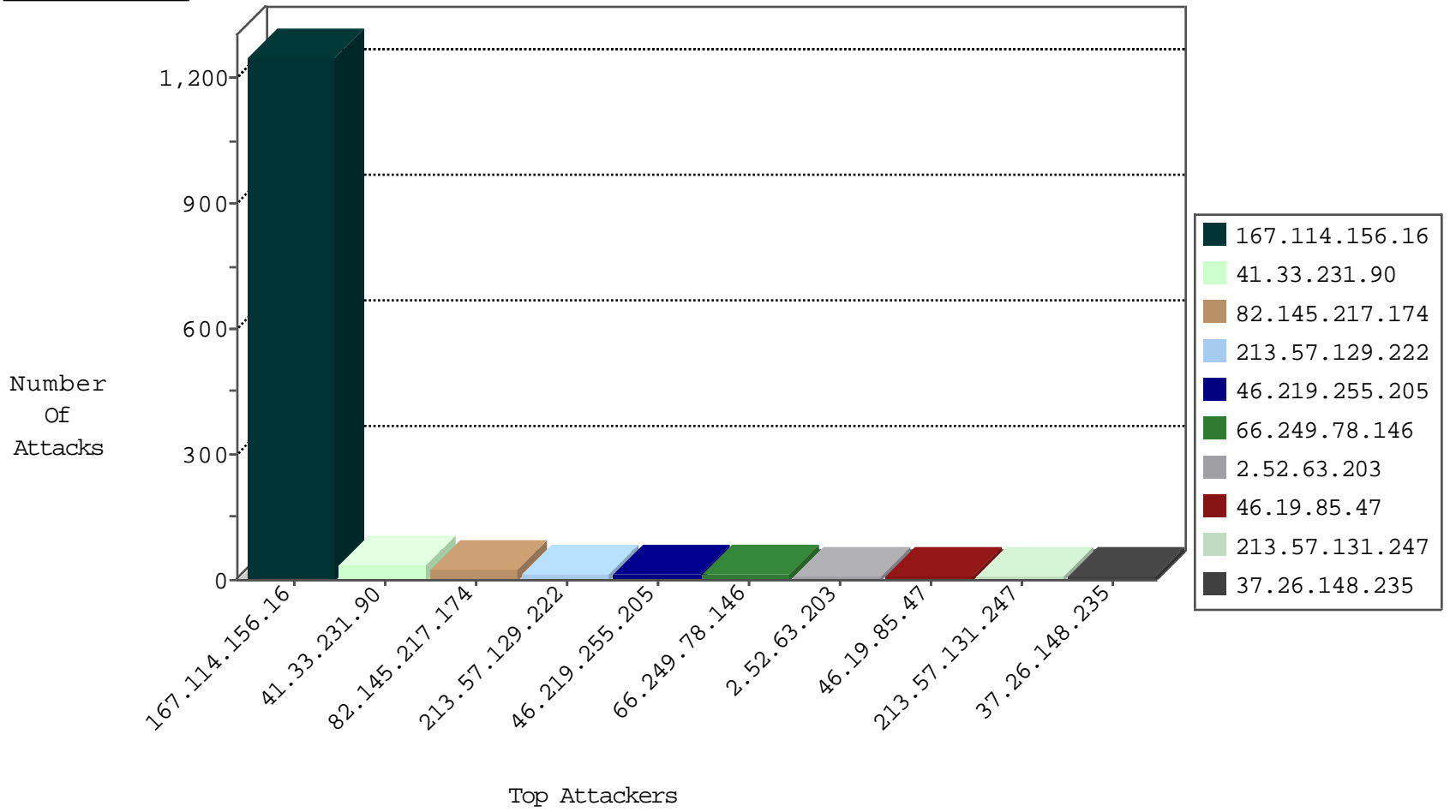
# IDF Under Attack Daily Report



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	3452
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.109.161.185		147.237.0.35	akaws.idf.il	I4 Source or Dest Port Zero	drop	1
125.86.166.172	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
125.86.166.172	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
213.204.101.24	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
115.231.209.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
115.231.209.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.66.199.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.129.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.177	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.214.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.170.36.188	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.219.255.205	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP admin.php access	1
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
158.69.222.199	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.231.209.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
115.231.209.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
104.143.14.247	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.177	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.177	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.219.255.205	147.237.77.233	Ukraine	atal.idf.il	SERVER-WEBAPP admin.php access	1
46.43.78.176	147.237.76.34	Palestinian Territory, Occupied	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
158.69.222.199	147.237.0.19	United States	madim.atal.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
82.145.217.174	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
172.56.41.213	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.109.166.206	Israel	147.237.76.86	navy.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	6
213.57.141.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.167.14	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.165.234.68	France	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.147.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.63.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
89.138.109.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.93.192	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.86.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.93.192	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
78.40.181.34	Lebanon	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
62.219.13.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.29.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	3
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.52.63.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
49.149.136.140	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.35.94.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.210.188.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.63.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
5.102.254.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.22	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.160.254.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.148.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.101	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.74	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
109.160.254.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.22.131.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.201	Israel	147.237.77.234	halag.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
109.64.157.187	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.25.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.165.234.68	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.165.234.68	Block	2
109.253.207.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.219.255.205	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.219.255.205	Block	2
46.219.255.205	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 46.219.255.205	Block	2
109.253.146.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.219.255.205	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	2
46.219.255.205	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
95.154.101.28	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation id in ww.idf.il/1294-en/dover.aspx	Block	1
46.166.186.197	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
193.90.12.87	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.177.159	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.177.159	Block	1
176.13.17.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.210.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.219.255.205	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	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
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.149	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.85.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.55.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.4.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.195.163	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/1133-22461-he/dover.aspx.	Block	1
46.210.229.89	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
5.28.151.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
176.13.19.69	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
149.88.90.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.219.255.205	Ukraine	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
109.67.153.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.62.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.24.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.10.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.197.165	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