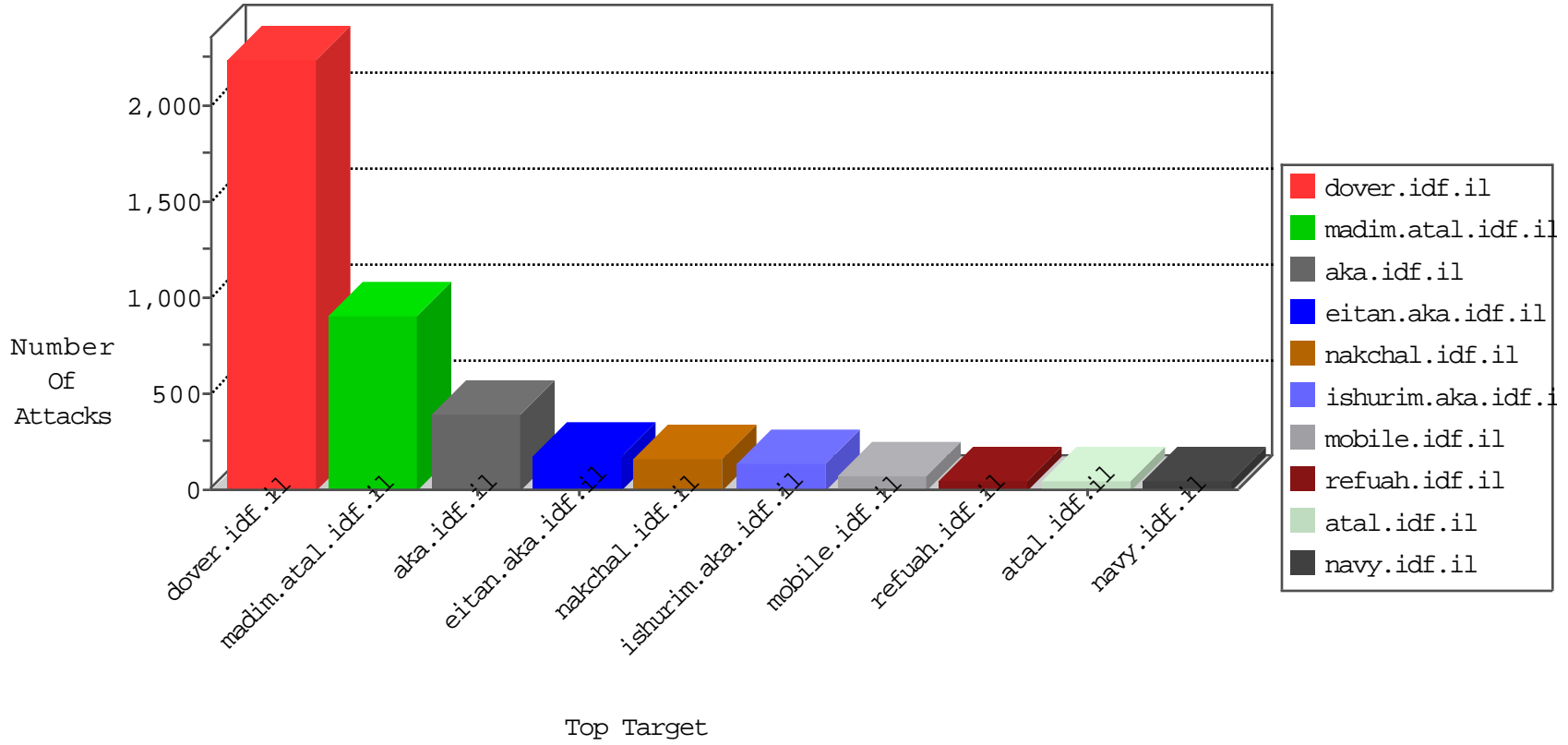


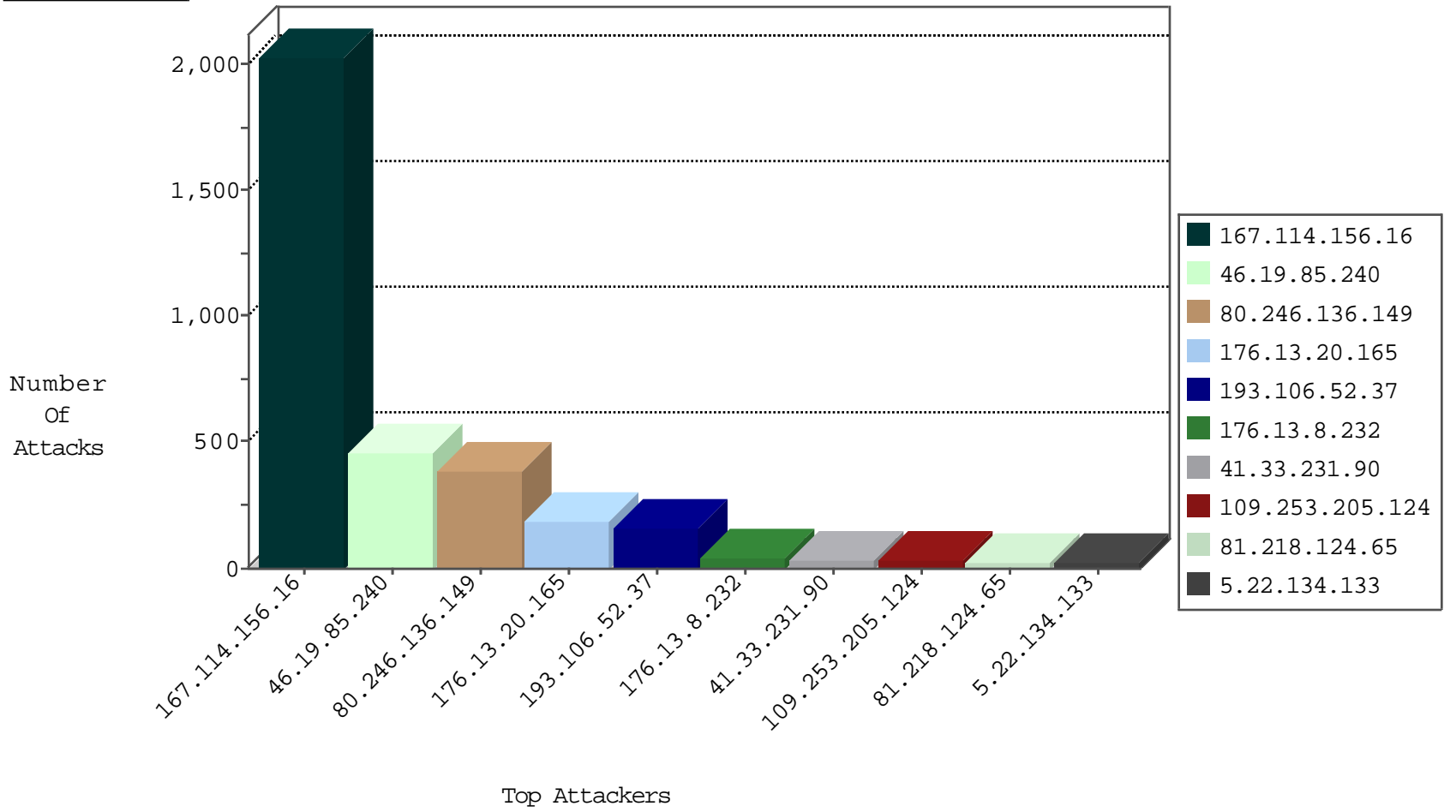
# IDF Under Attack Daily Report



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	3349
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	266
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
84.111.65.41	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.146.174	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
46.20.185.50	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

12-20-2015-10:04:08 to 12-20-2015-11:04:08

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	2
46.19.85.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.55.192.116	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.216	Sweden	dover.idf.il	ET SCAN NMAP -sS window 1024	1
123.196.116.66	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
84.94.79.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.55.192.116	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.132.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.217.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.196.116.66	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
93.173.45.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.190	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	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	30
81.218.124.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.253.205.124	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
213.57.143.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.222	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
79.179.216.242	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.52.179.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
31.168.137.30	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.177.55.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.198.151.37	Europe	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
5.22.134.133	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.48.37	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	12
31.168.76.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
79.177.55.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.5	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
81.218.48.37	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	9
80.178.187.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
113.77.40.16	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.54.134.79	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.147.0	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.198.22	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.22.134.133	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.178.208.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
5.22.134.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
82.80.42.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.111.65.41	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.182.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.198.151.37	Europe	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.42.174	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.20.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
176.13.20.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.48.37	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.114.23.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.36.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	221
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	180
176.13.20.165	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.20.165	Block	170
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	157
193.106.52.37	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
176.13.8.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.136.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.149	Block	4
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	4
79.182.12.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.130.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.33.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.17.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.183.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.194.111	France	147.237.77.74	law.idf.il	PHP Attempt	Block	2
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
193.106.52.37	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/images/shared/err_page.png	Block	2
2.54.158.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.194.111	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	2
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	2
176.13.19.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.237.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.148.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.110.106	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
195.154.194.111	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
50.62.176.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
192.114.38.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.170.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
91.231.192.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
176.13.8.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	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
31.168.137.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
109.65.182.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
195.154.146.225	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
2.54.149.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.47.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.17.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.162	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1