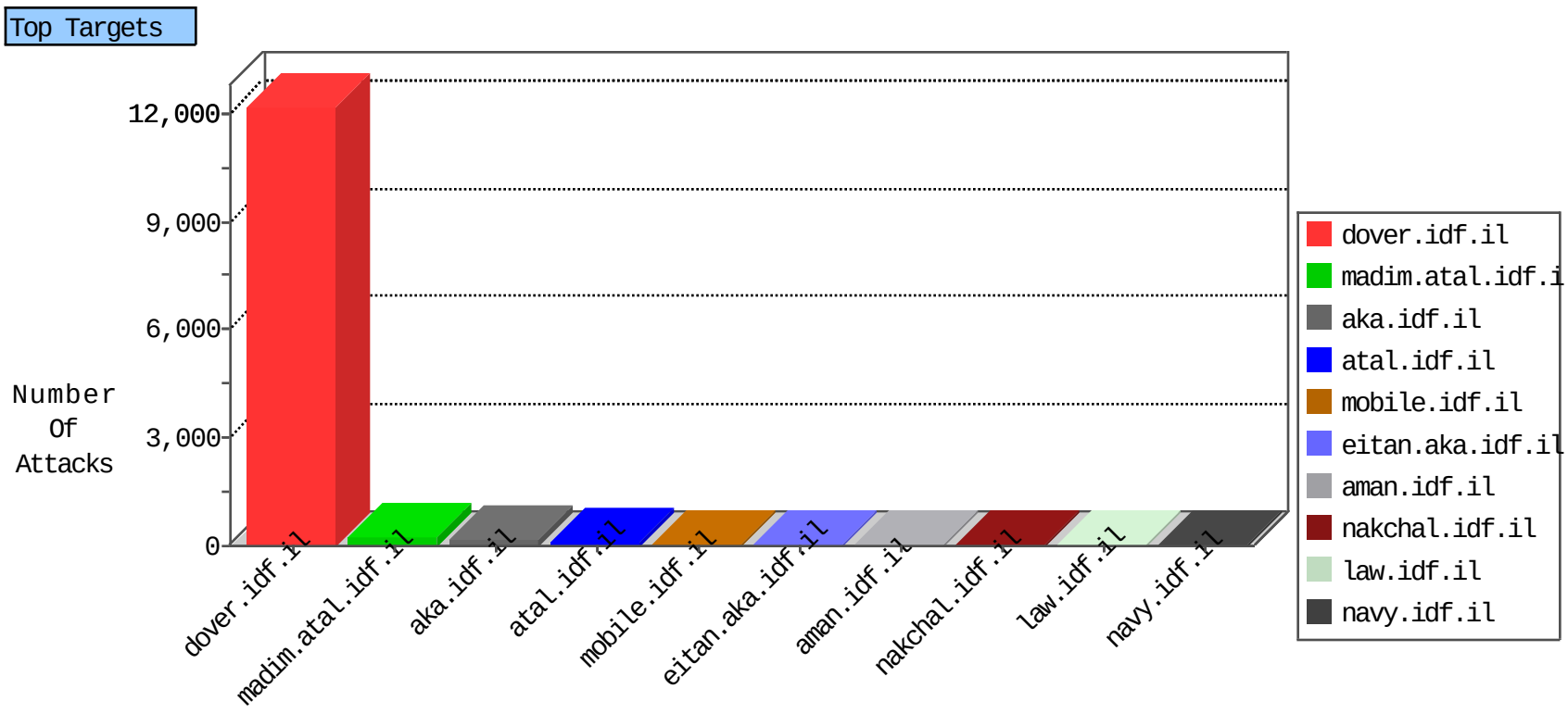
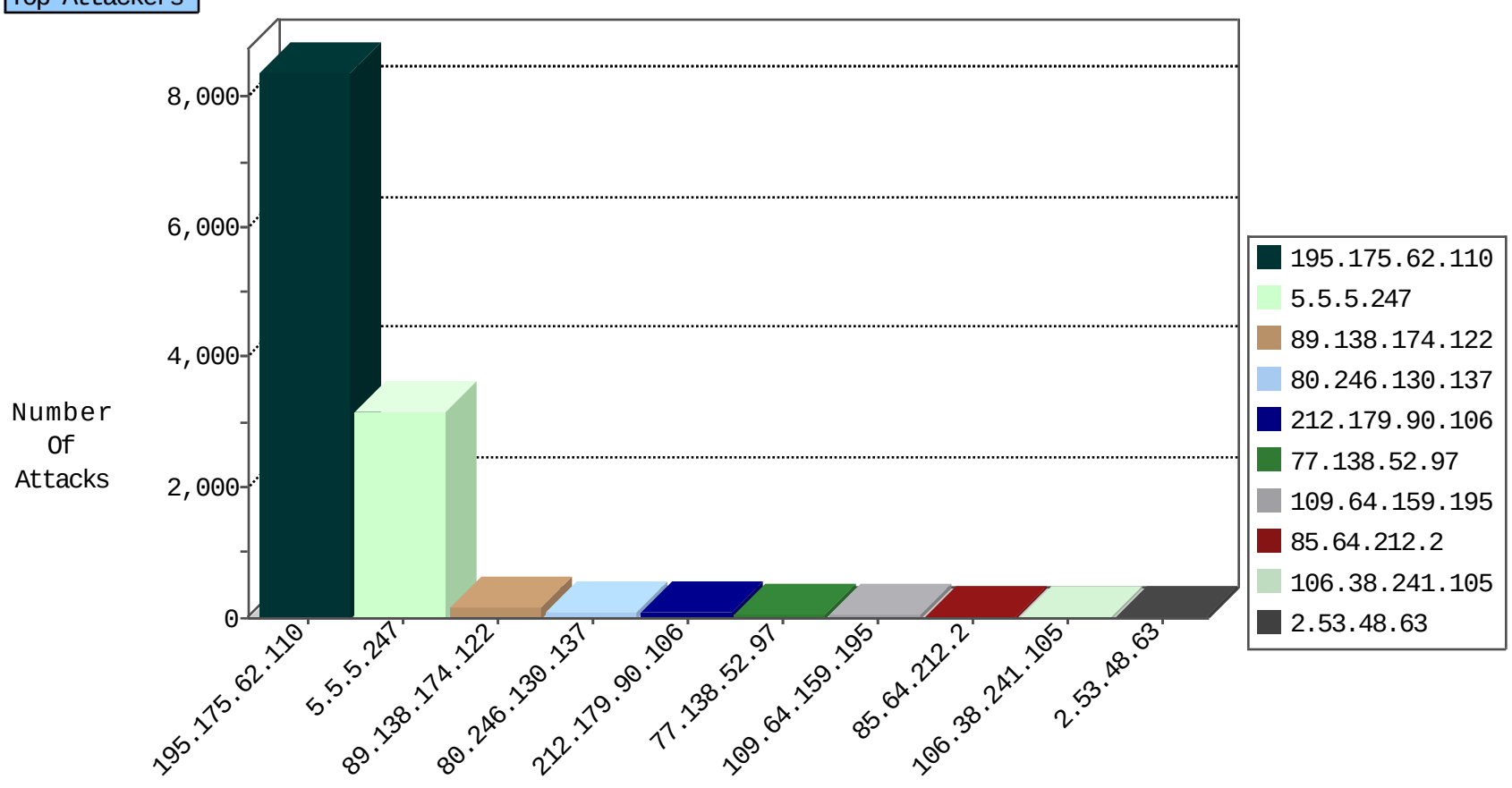
09-14-2016-23:04:01 to 09-15-2016-00:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-14-2016-23:04:01 to 09-15-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	137
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-23:04:01 to 09-15-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	8
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	7
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
69.30.234.186	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
69.30.234.186	United States	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.234.157.254	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-14-2016-23:04:01 to 09-15-2016-00:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.169.61	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.227.67.158	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.122.201.108	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.200.192.51	147.237.77.74	Brazil	law.idf.il	ET SCAN NMAP -sS window 3072	1
117.135.131.60	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
77.127.59.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.122.201.108	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.200.192.51	147.237.77.74	Brazil	law.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.52.71	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -f -sS	1

09-14-2016-23:04:01 to 09-15-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6210
5.5.5.247	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3160
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	726
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	501
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	287
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	206
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission		drop	156
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	SYN Attack		monitor	105
80.246.130.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	83
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	82
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	43
109.64.159.195	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.64.212.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	drop		drop	24
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
141.0.12.25	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
79.182.84.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.32.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
197.221.241.55	Zimbabwe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
156.204.206.138	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
93.83.18.6	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.3.147.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
89.139.153.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.69.6.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.10.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.139.153.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.16.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
2.53.158.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
151.224.238.247	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.246.133.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.195.163.123	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.195.163.123	Belgium	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-14-2016-23:04:01 to 09-15-2016-00:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.174.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
2.53.48.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
80.128.84.17	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
2.55.132.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.53.32.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.182.84.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.247.60	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
141.226.217.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
2.53.62.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.158.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	2
141.226.217.111	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	2
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2127-he/cogat.aspx	Block	1
46.19.86.77	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method uvc=1%7C37; in URL __atuvs=57d9baab0501a445000	Block	1
109.67.103.55	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.29.77.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method sdch in URL	Block	1
185.27.105.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.106.156	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
46.120.248.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyius	Block	1
141.226.217.111	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 141.226.217.111	Block	1
5.29.144.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.77	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	1
195.175.62.110	Turkey	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
80.246.130.137	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/63002.swf	Block	1
46.19.86.77	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version _pk_id.27.434e=c4ca8f9cf2eb4509.1473886894.0.1473886894..	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 198.161.119.4 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
95.86.121.155	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
2.55.56.249	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
79.178.98.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.18.213.246	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.93.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.77	Israel	147.237.76.86	navy.idf.il	Malformed URL __atuvs=57d9baab0501a445000;	Block	1
107.77.75.16	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/main/default.asp	Block	1
79.179.6.132	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
157.55.39.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
81.111.166.42	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1

09-14-2016-23:04:01 to 09-15-2016-00:04:01