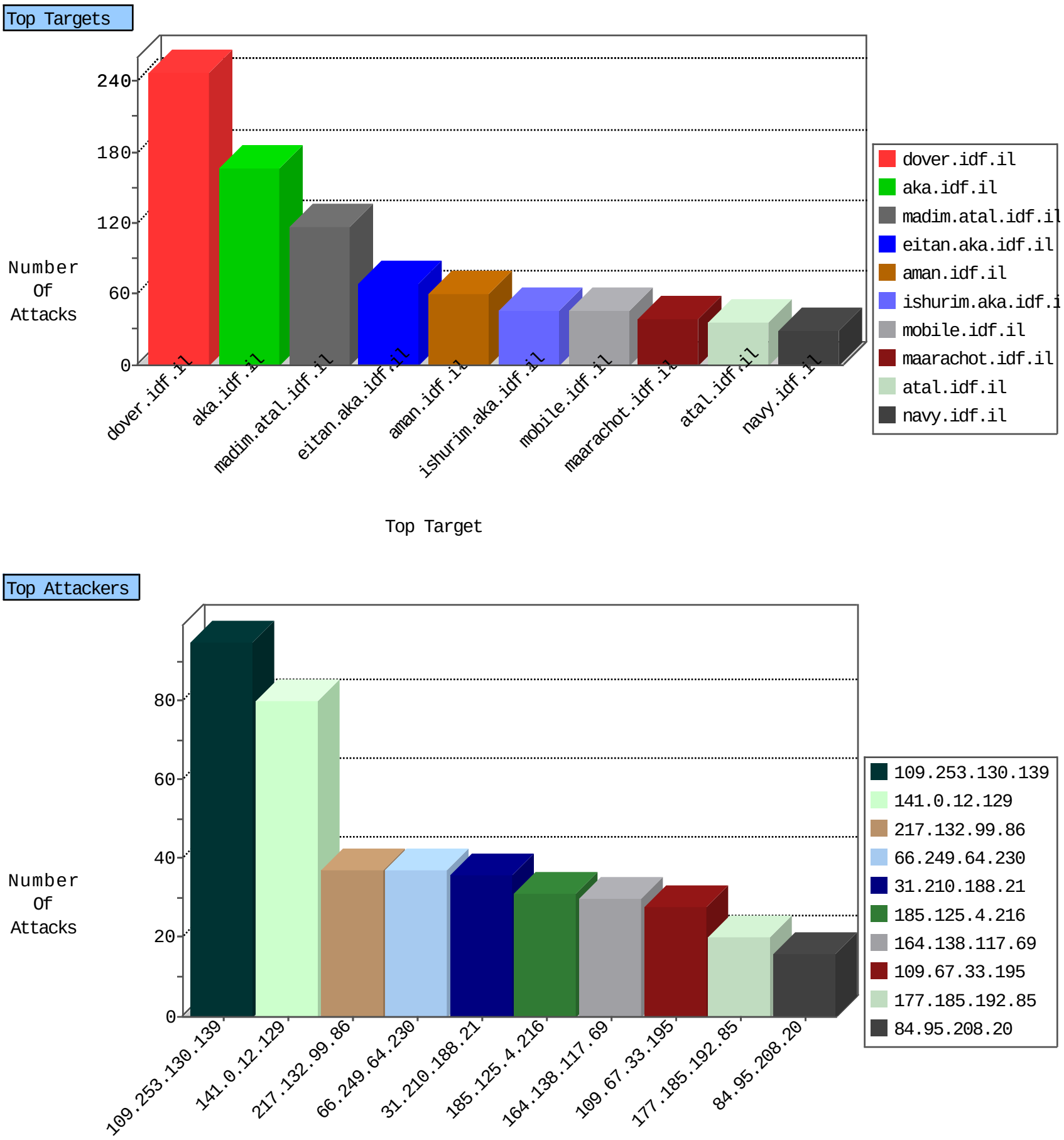
09-01-2016-16:04:00 to 09-01-2016-17:04:00

IDF Under Attack Daily Report



09-01-2016-16:04:00 to 09-01-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.85.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.253.208.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
37.26.148.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
207.46.13.8	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
31.168.81.160	Israel	147.237.72.166	aka.idf.il	Black List	drop	4
217.132.59.245	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
62.90.182.154	Israel	147.237.77.216	dover.idf.il	block-sp-traf1	forward	3
52.16.5.197	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	2
159.104.163.19	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
40.77.167.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
31.154.81.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
159.104.163.20	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.189.186.243	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.95.106	Netherlands	147.237.76.176	test.ncore.idf.i	Black List	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
159.104.163.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
216.243.31.2	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
159.104.163.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
5.189.186.243	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-01-2016-16:04:00 to 09-01-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-01-2016-16:04:00 to 09-01-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.230	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	37
177.185.192.85	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	20
209.222.4.188	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
109.67.48.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.123.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.14.48.62	147.237.77.216	Tunisia	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.32.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
185.120.124.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.146.112	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.83.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.143.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.61.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.99.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.248.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.135.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.12.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-01-2016-16:04:00 to 09-01-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.12.129	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.125.4.216	Poland	147.237.72.167	ishurim.aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	31
164.138.117.69	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
31.210.188.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
77.127.55.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.67.33.195	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
31.210.188.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
109.253.240.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.33.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
5.102.195.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.3.147.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
70.214.100.252	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
46.19.85.91	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.147.242	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
195.76.149.15	Spain	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
5.22.135.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.190	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
84.108.227.3	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
141.226.218.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.182	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.182	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.15.130.82	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.103.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.22.135.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.172.72	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.178.203.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
172.58.153.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
197.15.130.82	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.116.53.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.253.130.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.199.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.81.198	Europe	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.15.130.82	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.137.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.215.30	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
37.46.38.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.142.207	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.16.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
207.46.13.8	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.206.191	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
195.43.67.42	Poland	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2

09-01-2016-16:04:00 to 09-01-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.130.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
89.138.115.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	6
81.218.70.243	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
77.138.43.198	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.108.70.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.70.243	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/	Block	3
86.141.155.221	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
37.26.149.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.38.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.9.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
79.176.43.194	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.126.75.237	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.93.103	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.182.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.192.52	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.64.48	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
2.55.155.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16782-en/dover.a spx	Block	1
89.139.164.71	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.8.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
89.138.33.233	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.168.82.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
212.235.9.229	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.180.10.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.127.120.133	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
46.19.86.232	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.11.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.66.174.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
89.138.33.233	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 89.138.33.233	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
37.26.147.251	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
217.132.42.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-01-2016-16:04:00 to 09-01-2016-17:04:00