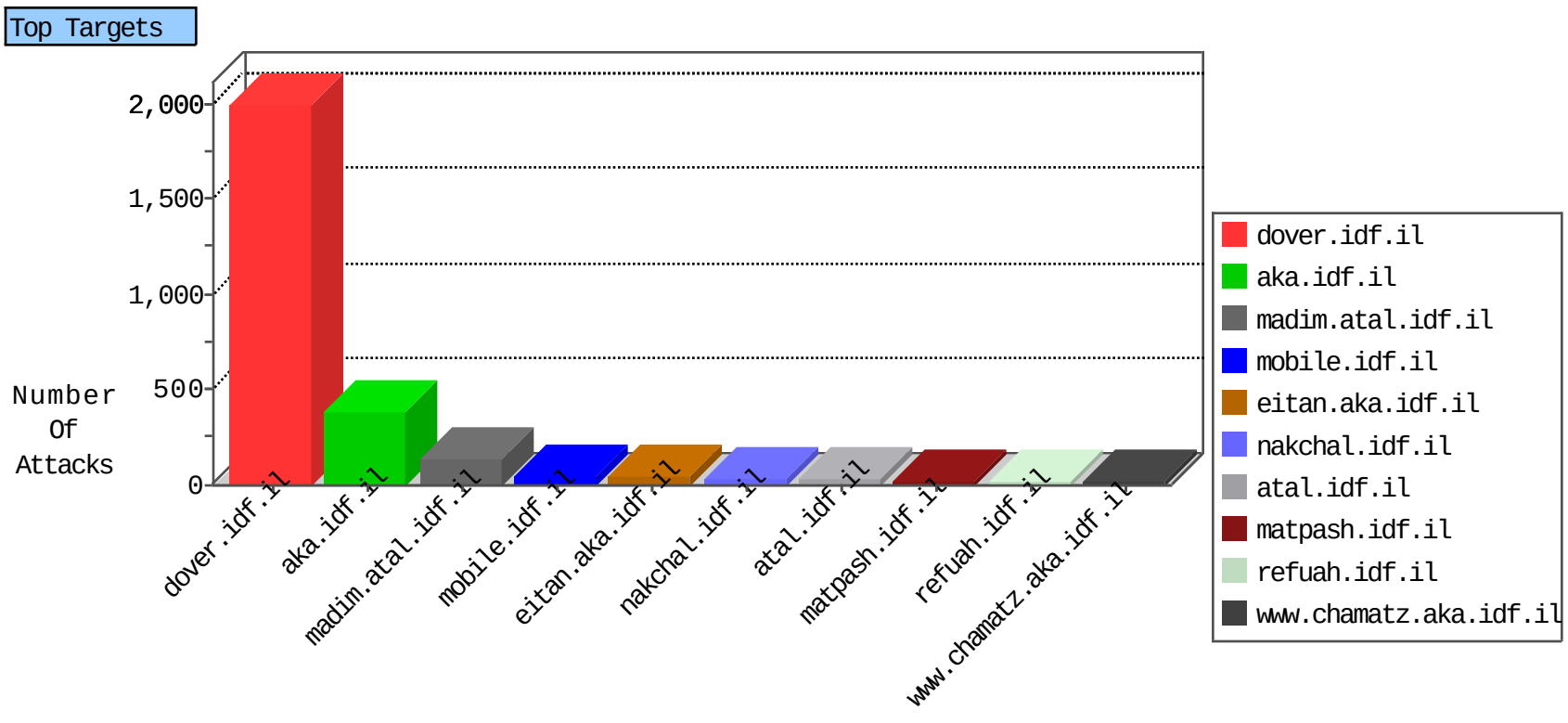
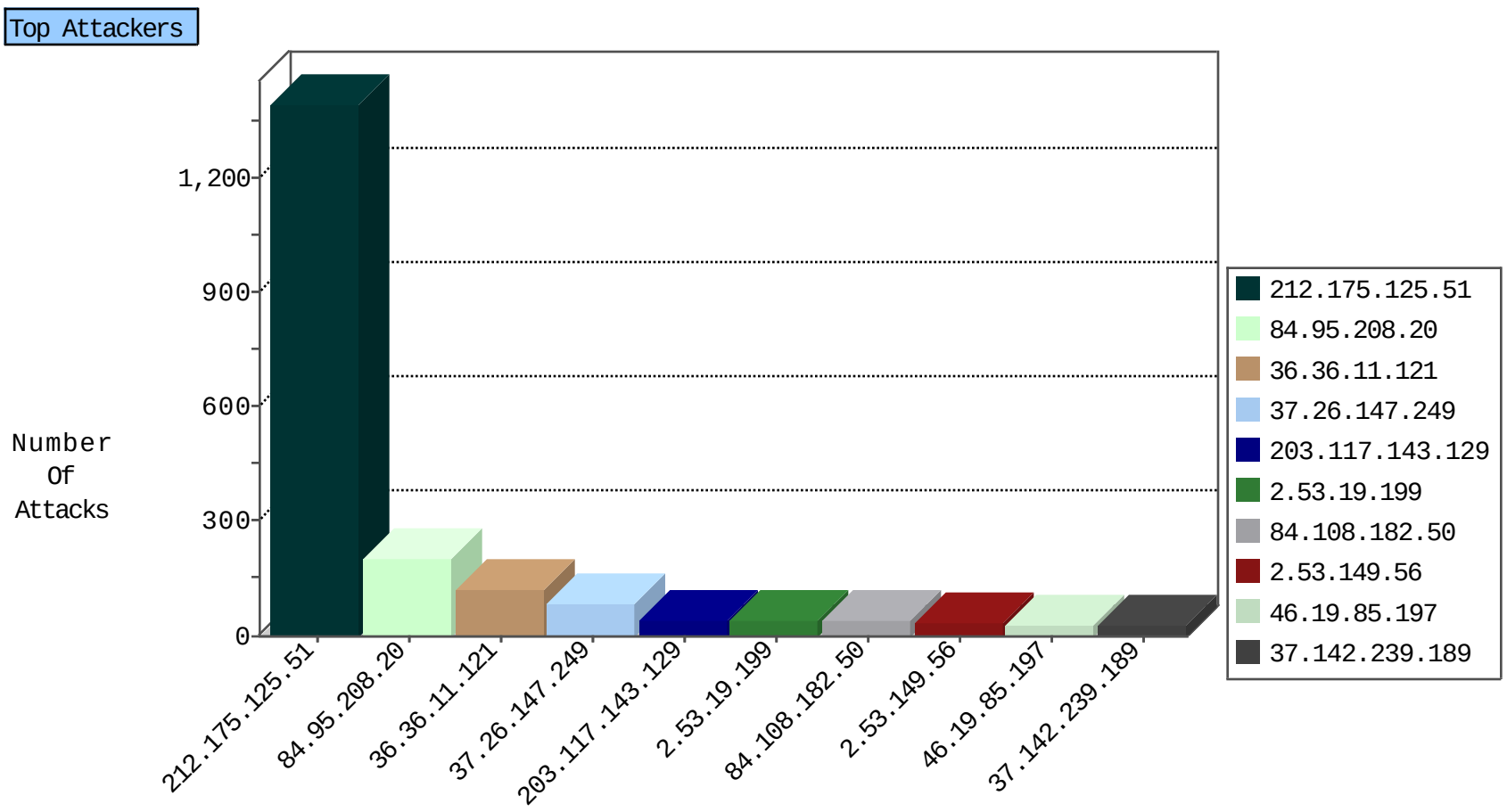
09-29-2016-12:04:06 to 09-29-2016-13:04:06

IDF Under Attack Daily Report





Top Attackers

09-29-2016-12:04:06 to 09-29-2016-13:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3280
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	223
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	86
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
46.19.85.197	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
198.44.110.12	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
213.151.48.8	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

09-29-2016-12:04:06 to 09-29-2016-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.247.61.153	Sweden	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	10
23.91.70.42	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.247.61.153	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
36.36.11.121	China	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
84.229.9.77	Israel	147.237.77.243	mobile.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-29-2016-12:04:06 to 09-29-2016-13:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.202.245	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
23.91.70.42	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
185.153.198.249	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.129.160.229	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
43.239.221.49	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Potential SSH Scan	1
176.13.12.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.59.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.237.121.146	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.13.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.36.97	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
193.104.115.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.161.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.129.160.229	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.239.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.40.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.56.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
134.191.232.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.5.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.76.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.171.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-12:04:06 to 09-29-2016-13:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1193
36.36.11.121	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
212.175.125.51	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	50
203.117.143.129	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
2.53.149.56	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.142.239.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
176.37.8.116	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.195.21	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.181.223.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.209.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.134.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.169.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
105.155.131.118	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.118.36.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.205.58	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	6
46.19.85.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.195.162.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.205.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.175.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
141.226.217.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.116.108.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
61.247.254.226	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
92.207.147.87	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.116.53.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.36.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
119.81.247.109	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.71.17.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
93.172.125.55	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.156.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.226.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.235.34.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.205.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4

09-29-2016-12:04:06 to 09-29-2016-13:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	127
37.26.147.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	42
2.53.19.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	38
79.178.145.182	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.145.182	Block	24
193.169.204.11	Germany	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	18
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	17
175.44.35.170	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 175.44.35.170	Block	15
5.29.115.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.115.122	Block	13
175.44.35.170	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
193.169.204.11	Germany	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	6
109.253.146.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
192.116.232.69	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	4
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	4
77.138.67.130	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
79.181.200.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.208.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.68.124	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/112326.pdf	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	3
176.13.240.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.232.154	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
109.253.202.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.154.170	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	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
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	2
79.178.145.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/71772.pd	Block	1
2.53.164.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
66.249.66.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22714-ar/dover.aspx	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
77.139.102.34	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in URL	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71616.pdf	Block	1
213.8.204.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71709.pdf	Block	1
185.89.217.227	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/	Block	1
37.26.149.198	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.170.134	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
66.249.66.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_sto	Block	1
83.166.241.14	Russian Federation	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
176.13.246.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.168.68.124	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 31.168.68.124	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method žé¡³Vˆb in URL	Block	1

09-29-2016-12:04:06 to 09-29-2016-13:04:06