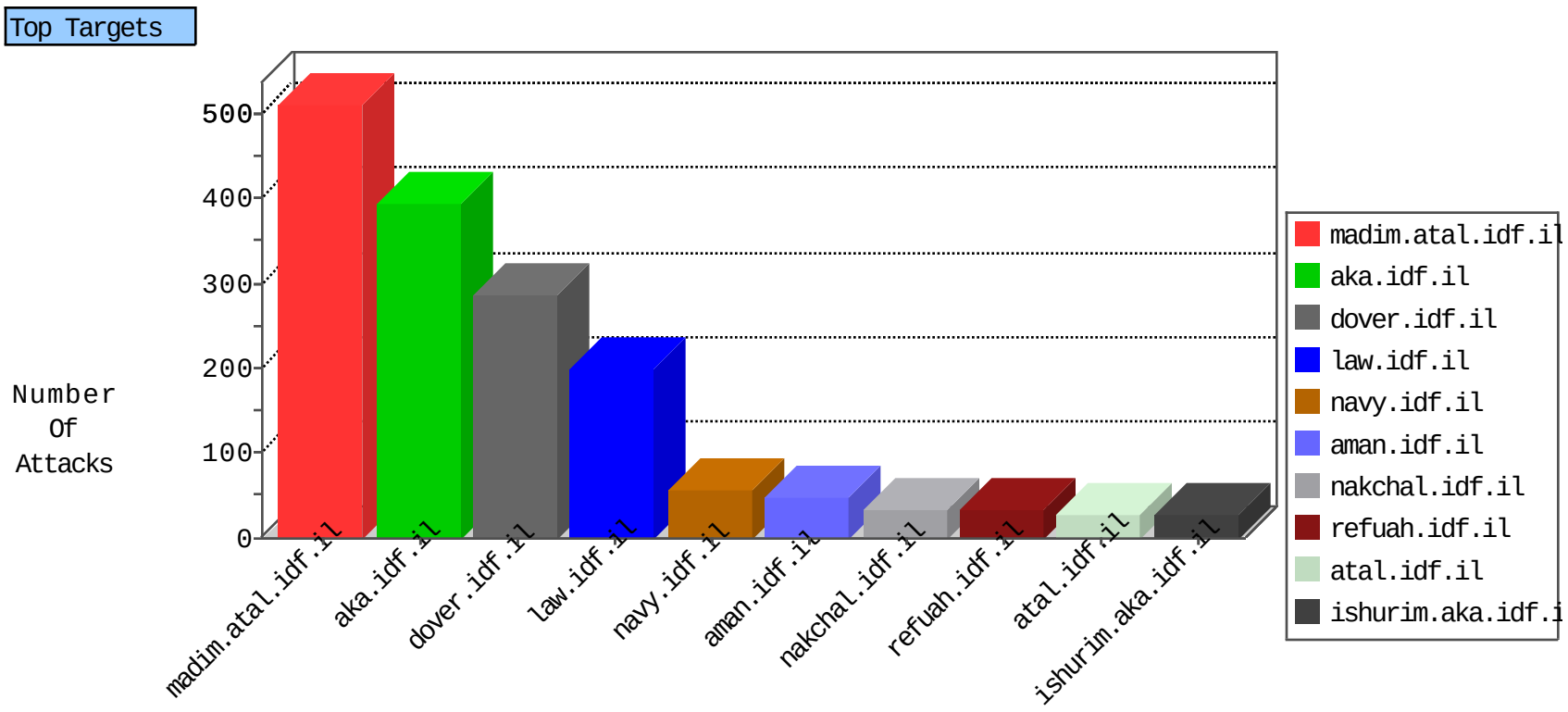
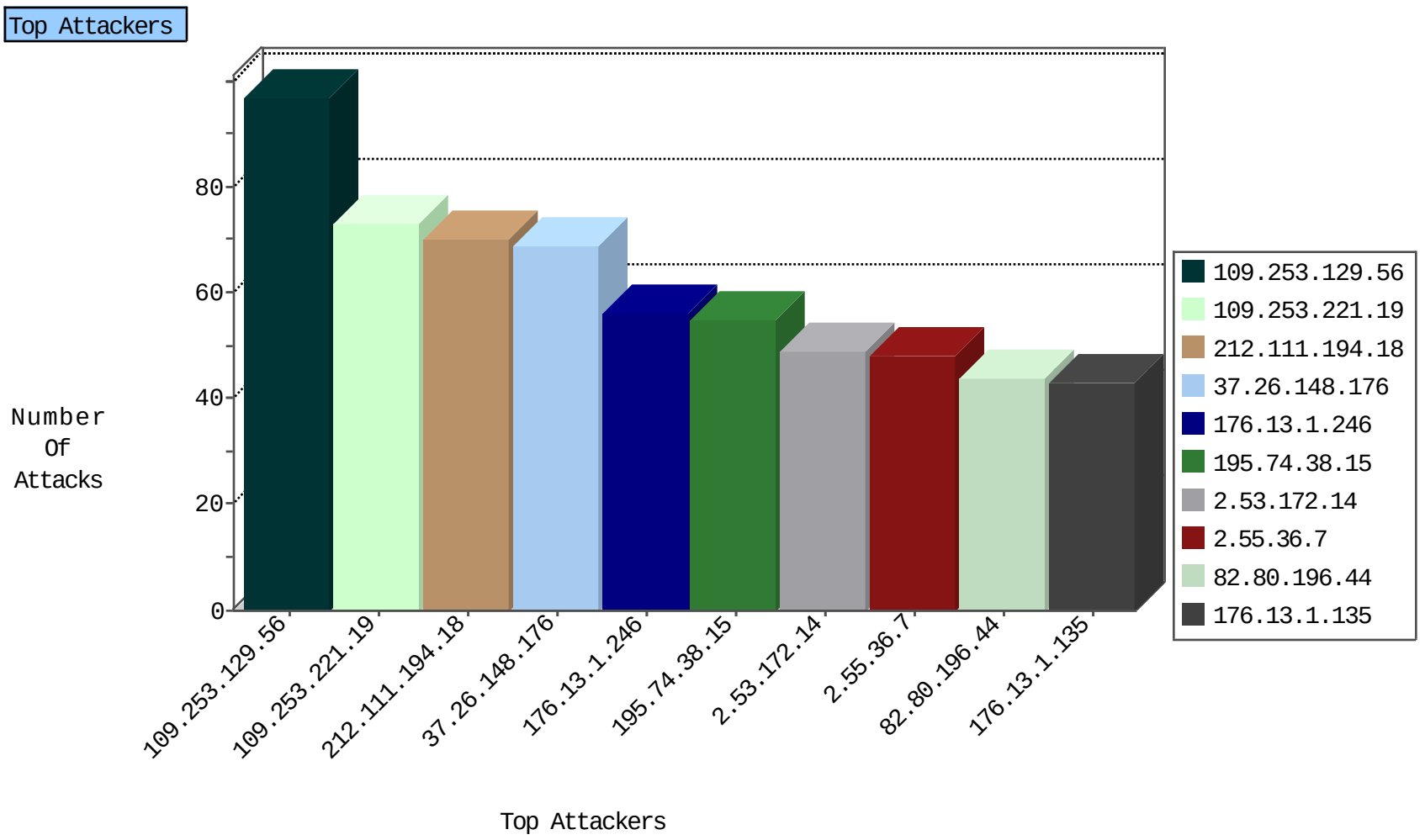
09-18-2016-11:04:07 to 09-18-2016-12:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-18-2016-11:04:07 to 09-18-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
82.80.190.111	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
193.1.13.14	Ireland	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
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.156	aman.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
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.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
156.56.250.227	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
37.26.147.146	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.217	e.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

09-18-2016-11:04:07 to 09-18-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.74.38.15	Sweden	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
212.111.194.18	Ukraine	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
97.74.215.165	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.26.128.28	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.111.194.18	Ukraine	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.74.38.15	Sweden	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.86.161.214	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
192.169.249.95	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
212.111.194.18	Ukraine	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	4
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.119.125.57	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.74.38.15	Sweden	147.237.76.86	navy.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	3
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.91.70.51	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2
158.85.253.245	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
24.86.161.214	Canada	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
192.116.160.17	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
125.64.94.206	China	147.237.72.166	aka.idf.il	C1000003: HTTP: phpMyAdmin access	Permit	1
192.169.249.95	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-18-2016-11:04:07 to 09-18-2016-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.1.246	147.237.77.216	Israel	dover.idf.il	GPL SCAN nmap TCP	55
212.111.194.18	147.237.77.74	Ukraine	law.idf.il	SQL Injection - Select From	52
195.74.38.15	147.237.76.86	Sweden	navy.idf.il	SQL Injection - Select From	36
24.86.161.214	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	19
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
216.26.128.28	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
97.74.215.165	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	17
216.119.125.57	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
192.169.249.95	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	11
162.248.76.109	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.2.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.79.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.125.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.248.76.109	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
162.248.76.109	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
62.219.227.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	1

09-18-2016-11:04:07 to 09-18-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.221.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
89.139.201.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
89.139.201.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
62.0.200.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
84.108.17.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
192.115.163.105	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
185.32.179.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.234.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.32.179.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.7.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.156.240.147	Spain	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.182	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.209.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
109.253.200.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.231.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
217.194.199.223	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.178	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.178	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.242.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	4
109.67.253.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.7.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.172.14	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.135.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.25.102.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.55.149.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.37.49	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	4
2.53.21.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.186	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.46.38.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
217.194.197.141	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.94.120.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-18-2016-11:04:07 to 09-18-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
109.253.221.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
37.26.148.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
2.55.36.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
176.13.1.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.53.172.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
37.26.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.85.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.14.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.53.37.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.53.146.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
212.150.195.192	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	10
5.29.202.152	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	5
77.138.127.250	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	5
125.64.94.206	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 125.64.94.206	Block	4
176.13.4.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.145.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
109.253.194.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.38.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.193.51.38	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	3
2.55.137.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.19.86.149	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.139.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.172.14	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.197.83	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.222.204	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
62.219.114.38	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.222.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
91.193.51.38	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.193.51.38	Block	2
217.194.199.223	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
85.64.146.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.6.132	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
175.123.98.240	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/manager/html	Block	1
46.19.86.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.215.168	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.167.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.140.163	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
217.194.202.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.204.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.15.227	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.222.164	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
37.142.250.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1

09-18-2016-11:04:07 to 09-18-2016-12:04:07