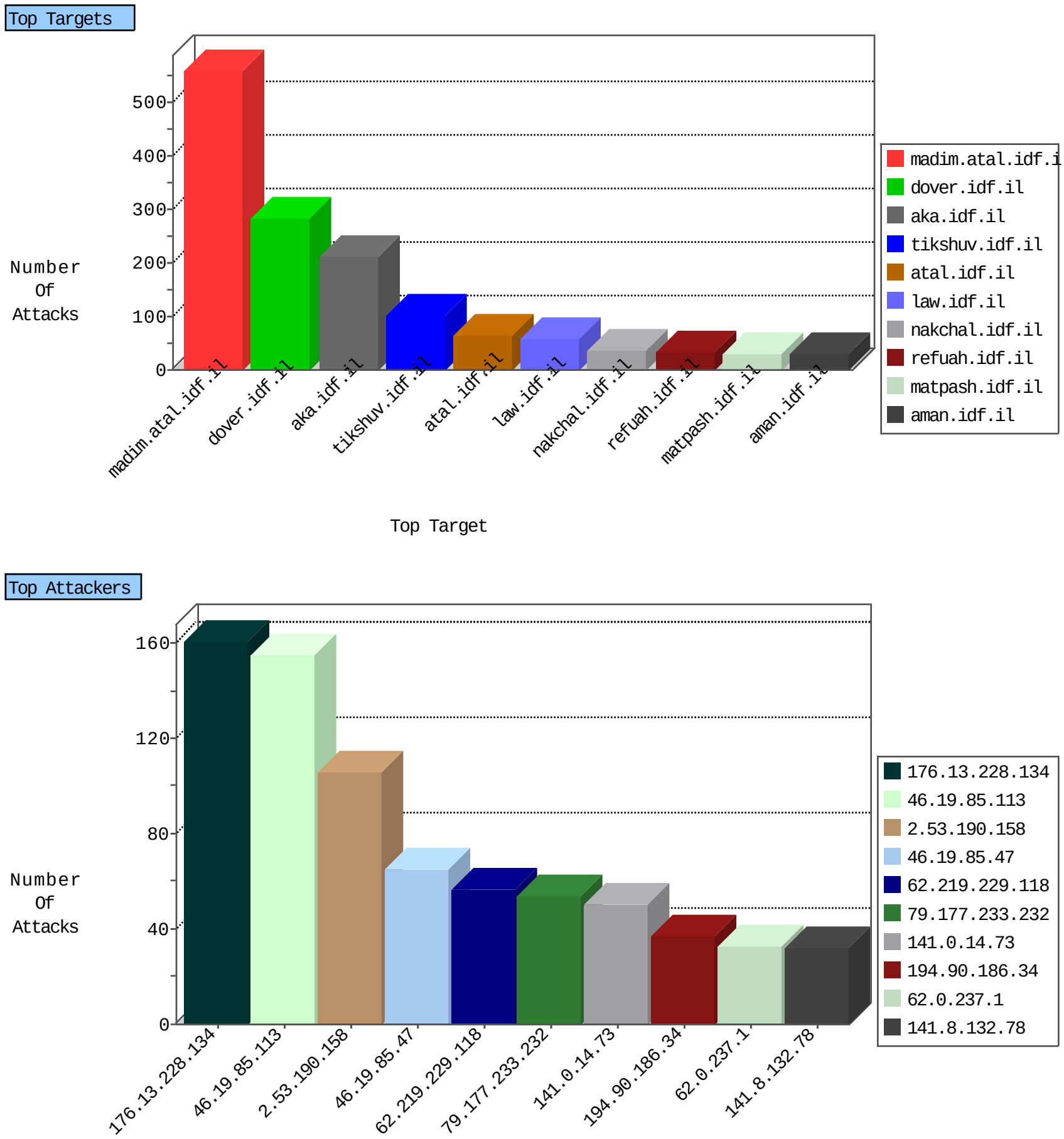
09-13-2016-09:04:00 to 09-13-2016-10:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers

09-13-2016-09:04:00 to 09-13-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.150.127.133	Israel	147.237.77.216	dover.idf.il	ICMP-Frag-Needed-Storm	drop	16
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
82.80.217.70	Israel	147.237.77.170	maarachot.idf.il	Black List	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	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	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
213.8.122.57	Israel	147.237.72.156	aman.idf.il	Black List	drop	1
198.82.160.221	United States	147.237.72.166	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
128.223.8.114	United States	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
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	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
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.14	dover.idf.il(old)	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
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-09:04:00 to 09-13-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
119.75.47.122	Singapore	147.237.77.216	dover.idf.i	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-13-2016-09:04:00 to 09-13-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.219.229.118	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	57
46.120.122.219	147.237.76.31	Israel	nakchal.idf.il	Xenu Link Sleuth User Agent	2
5.255.90.133	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.227.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.100.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
86.58.69.133	147.237.76.38	Slovenia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.154.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.64.166	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
31.168.133.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.62.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
147.235.185.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.50	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
82.81.29.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.197.195	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.87	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.18.21.64	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1

09-13-2016-09:04:00 to 09-13-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.73	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
194.90.186.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.47	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
77.127.59.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.116.76.210	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
46.19.85.47	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.178.204.23	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.72.103.229	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
2.55.170.59	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.164	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.235.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.122	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.122	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.250.156.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
194.90.66.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
176.65.18.110	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.161.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.0.217.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.107	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.51.3	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
81.218.57.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
188.120.154.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.130.38	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.155.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.251.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
114.37.243.5	Taiwan	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
2.53.26.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.38.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
62.0.219.129	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
213.57.166.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-13-2016-09:04:00 to 09-13-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.228.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
2.53.190.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
79.177.233.232	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	27
109.253.201.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
79.177.233.232	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.177.233.232	Block	26
79.180.32.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
140.207.223.183	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 140.207.223.183	Block	15
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
2.53.159.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.197.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
88.202.218.243	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
140.207.223.183	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
2.53.129.65	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.139.48	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	6
109.253.137.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.6.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.204	Israel	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/error.htm parameter aspxerrorpath	Block	2
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 213.151.32.163	Block	2
46.19.86.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.13	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
217.132.61.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.168.101.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
212.179.132.204	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
176.13.228.134	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
80.179.223.150	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
213.57.105.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
77.127.59.137	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
2.53.190.158	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
82.166.100.163	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
80.246.136.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.84.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
140.207.223.183	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
84.108.121.190	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.233.232	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.en/general/	Block	1
194.90.186.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.117.59.132	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1678	Block	1
77.138.202.217	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
46.19.86.164	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.207	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1

09-13-2016-09:04:00 to 09-13-2016-10:04:00