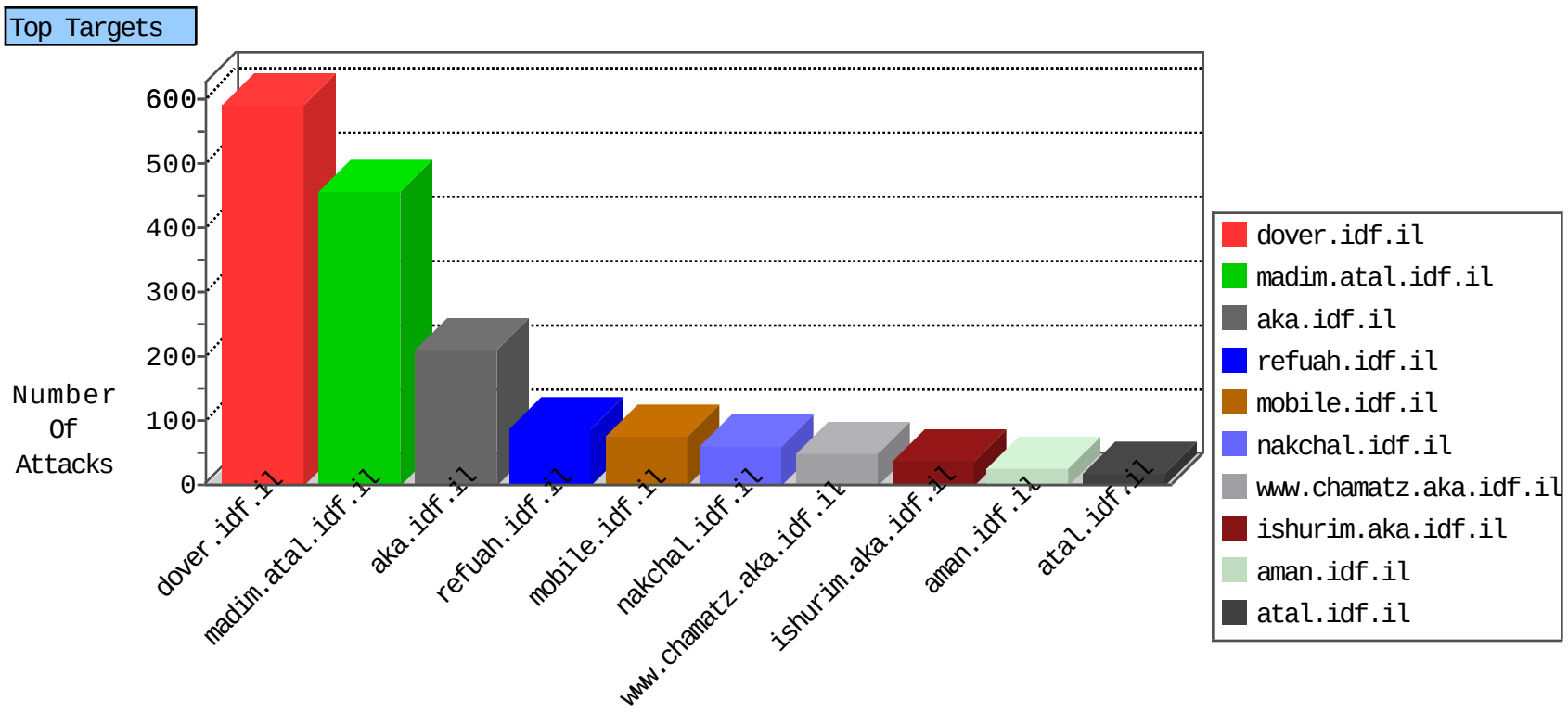
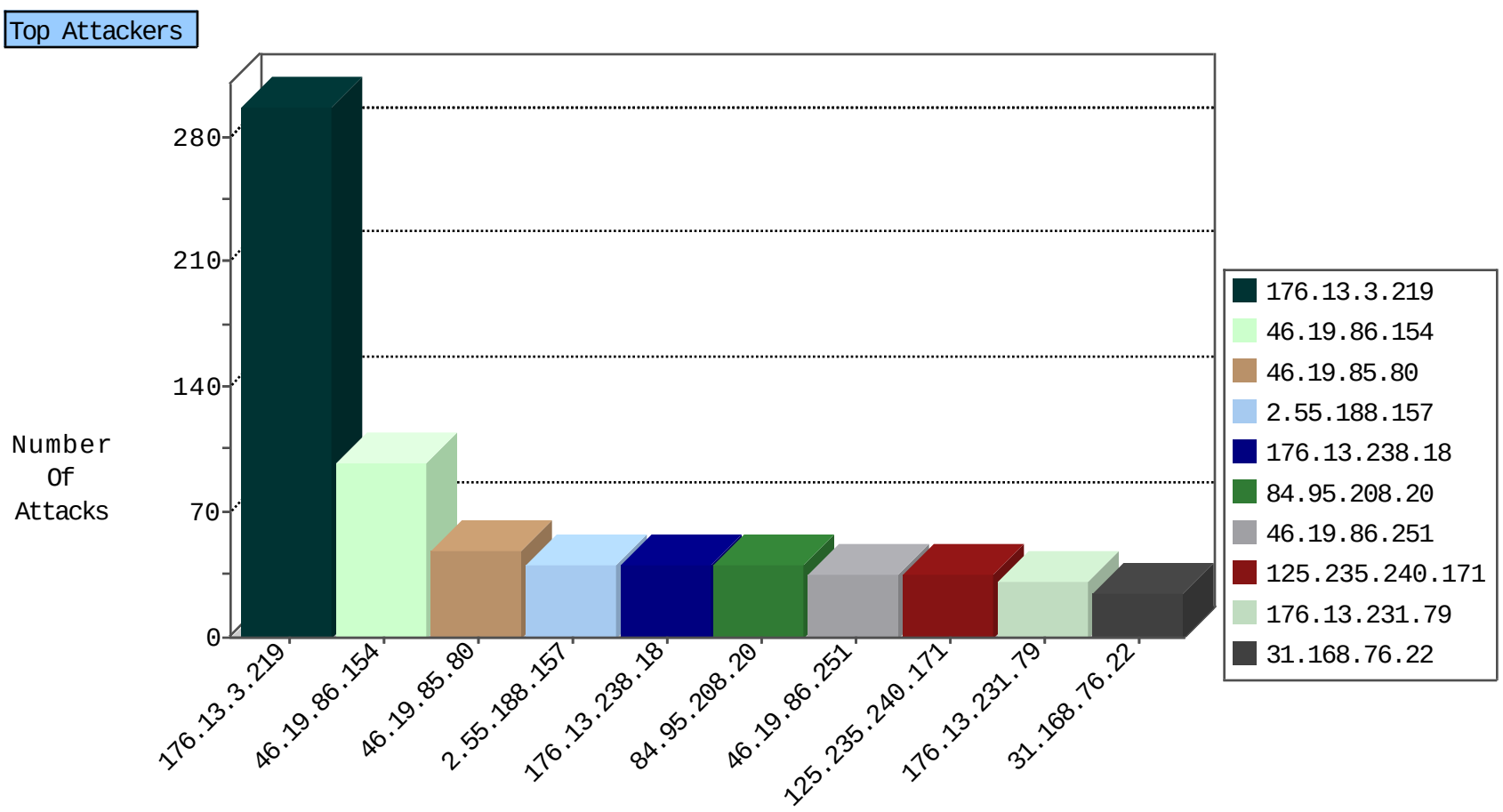
09-28-2016-09:04:02 to 09-28-2016-10:04:02

IDF Under Attack
Daily Report





09-28-2016-09:04:02 to 09-28-2016-10:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
31.168.204.250	Israel	147.237.77.216	dover.idf.il	Black List	drop	8
31.168.204.250	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	4
2.53.183.253	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
173.208.150.114	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.30.193.251	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.213.196	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
63.141.242.194	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
192.187.118.69	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
173.208.213.198	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
198.204.255.74	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
77.138.52.97	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
63.141.231.195	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
142.54.174.83	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
63.141.242.195	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.12.217.6	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.207.133	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
91.230.121.156	Ukraine	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
63.141.231.211	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
192.187.109.61	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
93.158.200.206	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
142.54.180.68	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
69.30.227.219	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
93.158.200.206	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
63.141.242.195	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

09-28-2016-09:04:02 to 09-28-2016-10:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
5.189.190.238	Germany	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

09-28-2016-09:04:02 to 09-28-2016-10:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.175.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.135.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.6.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.210.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.220.2.5	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.76.102.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.193.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.135.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.6.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.150.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.122.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.236.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.25.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.79.2.19	147.237.0.19	Australia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.117.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.226.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.223.94.128	147.237.77.176	Bolivia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.189.190.238	147.237.0.15	Germany	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
149.255.108.192	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-28-2016-09:04:02 to 09-28-2016-10:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
125.235.240.171	Vietnam	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
176.13.231.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.66.53.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.86.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
62.0.222.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.188.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	11
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
176.13.237.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.188.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
174.44.72.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.48.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.238.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
80.246.138.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.210.235.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.0.212.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.238.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.74.107.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.188.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
207.232.45.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.25.69.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
185.3.147.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.3.219	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
176.13.238.18	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
2.53.55.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.188.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
109.253.132.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.138.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.210.235.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
213.241.16.169	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.76.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.183.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.133.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.193.36	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
31.168.76.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

09-28-2016-09:04:02 to 09-28-2016-10:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	276
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
37.26.147.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
62.90.139.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
176.13.231.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
77.124.25.205	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 77.124.25.205	Block	5
176.13.3.219	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
194.90.200.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.200.70	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
32.42.29.204	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 32.42.29.204	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
62.90.139.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.48.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
32.42.29.204	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	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
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.116.213.179	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.213.179	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
31.168.144.11	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
178.162.216.32	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
66.249.69.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3470.jpg	Block	1
62.219.145.163	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/801-he/patzar.aspx	Block	1
37.26.148.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.50.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
54.210.70.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
180.76.15.18	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.69.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
80.246.133.77	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
2.53.144.9	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
85.64.33.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.179	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
62.90.139.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.90.139.206	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
138.201.59.34	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1

09-28-2016-09:04:02 to 09-28-2016-10:04:02