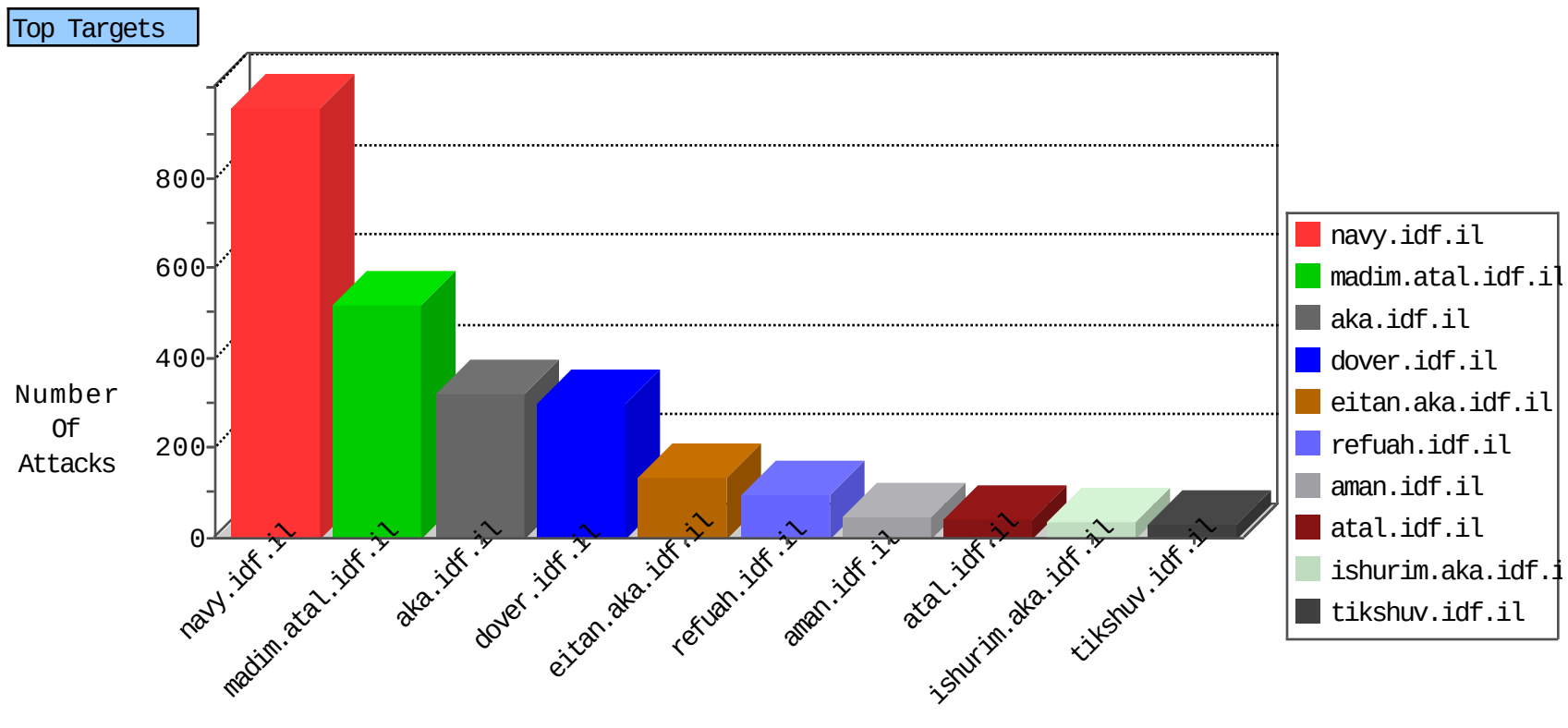
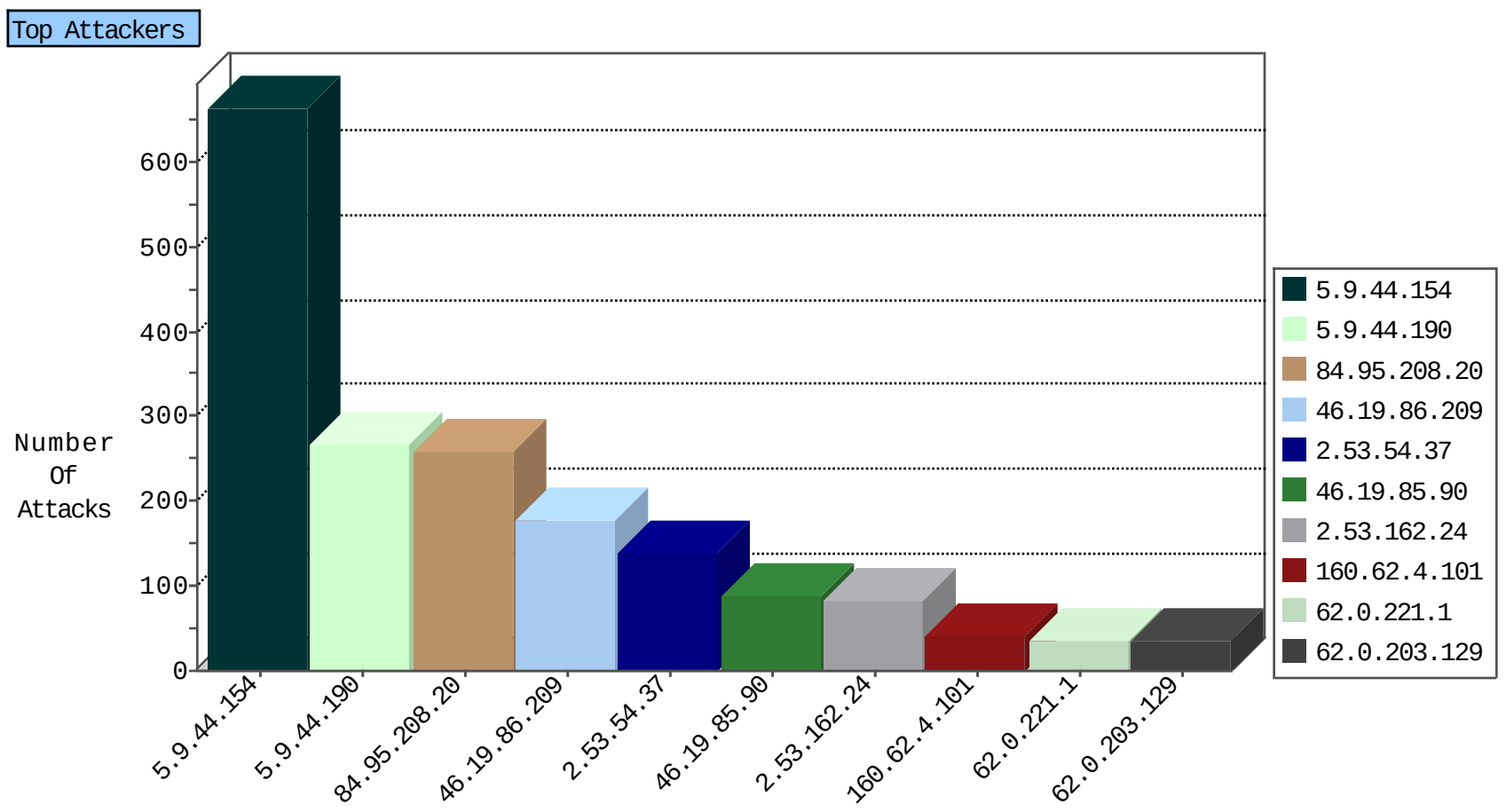
09-11-2016-11:04:09 to 09-11-2016-12:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
212.179.1.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
82.80.217.70	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
77.139.152.93	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.146.194	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.65.4.192	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1
62.90.220.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.106	France	147.237.76.42	refuah.idf.i	C1000146: HTTP: AhrefBot crawler	Block	1
199.87.254.47	United States	147.237.77.216	dover.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
199.87.254.195	United States	147.237.77.74	law.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.146.194	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
94.188.155.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.33.38.37	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.157.86.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.53	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.69.148.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.53	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.144.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.53	147.237.72.156	United States	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.0.102.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.206.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.41.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.3.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.158.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.5.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.244.23.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.64.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
168.1.128.53	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.130.235.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.53	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.125.26.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.53	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
141.226.217.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.103.178	147.237.76.86	United States	navy.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
109.253.136.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.92.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.48.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.52.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.180.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack		monitor	333
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	282
5.9.44.190	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	164
5.9.44.190	Germany	147.237.76.86	navy.idf.il	SYN Attack		monitor	94
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	45
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
160.62.4.101	Switzerland	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	41
62.0.221.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
62.0.209.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
91.135.102.162	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
91.135.102.162	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
46.19.85.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.138.12	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
95.35.201.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.129.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.92.5.82		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.9.44.190	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.69.52.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.8.188	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.237.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
95.35.201.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.199.163	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.211.129	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
212.199.57.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
95.35.201.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.54.199.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.137	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
219.134.63.89	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.146.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.137	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
37.142.8.201	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	178
2.53.54.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	109
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	85
2.53.162.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
109.253.222.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
37.26.146.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
77.138.232.143	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	3
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	2
80.246.137.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.52.62	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	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
80.246.139.207	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.8.178	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.137.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.145.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.143.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.131	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.238.139	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.156.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
5.29.76.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
202.66.60.168	Hong Kong	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.143.101	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
80.246.138.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.46.38.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.10.21	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
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
37.26.146.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.251.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
2.53.176.124	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
82.80.198.164	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
185.32.179.140	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.197.93	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspxa	Block	1
37.26.148.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.109.50	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.176	Block	1
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
204.79.180.33	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
2.53.157.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.240.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.10.21	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.181.10.21	Block	1
68.180.230.107	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

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