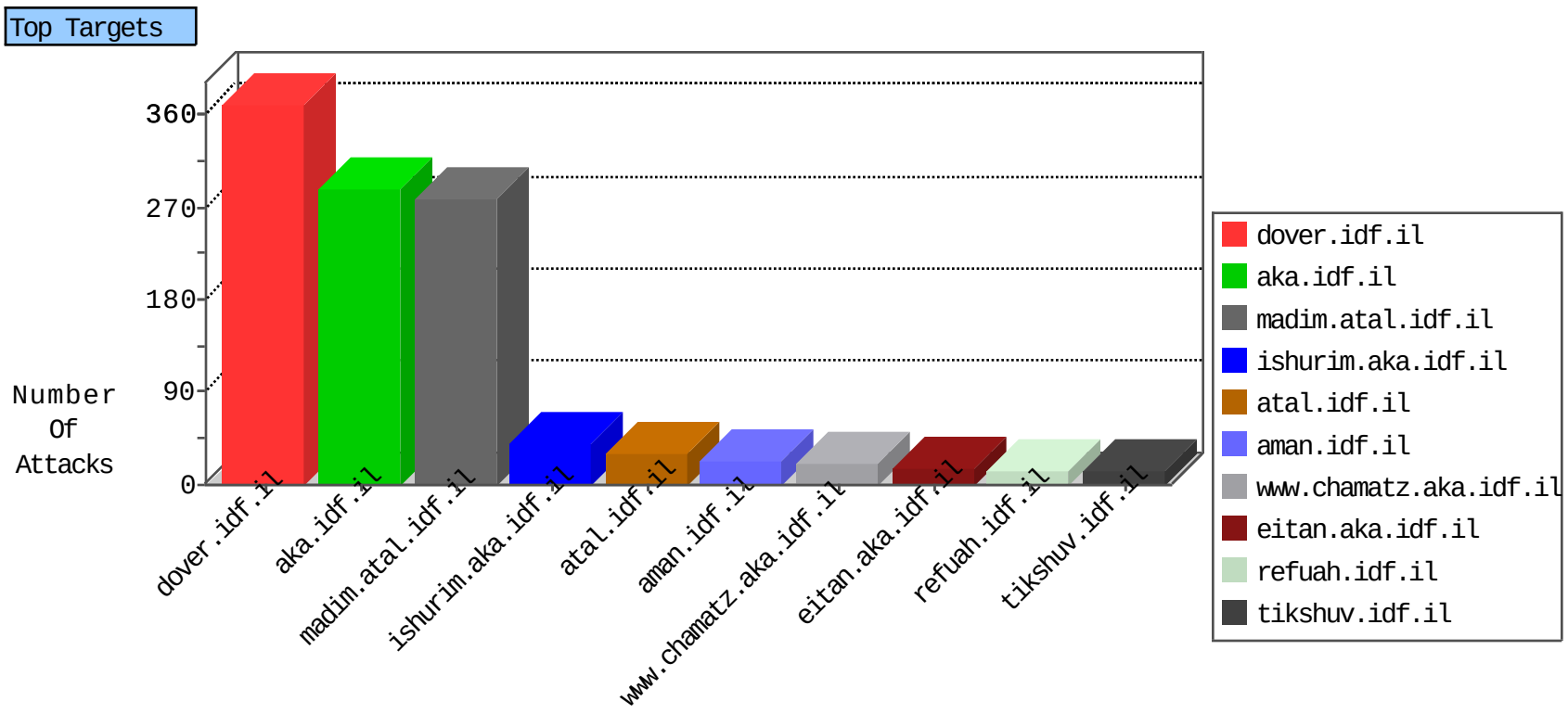
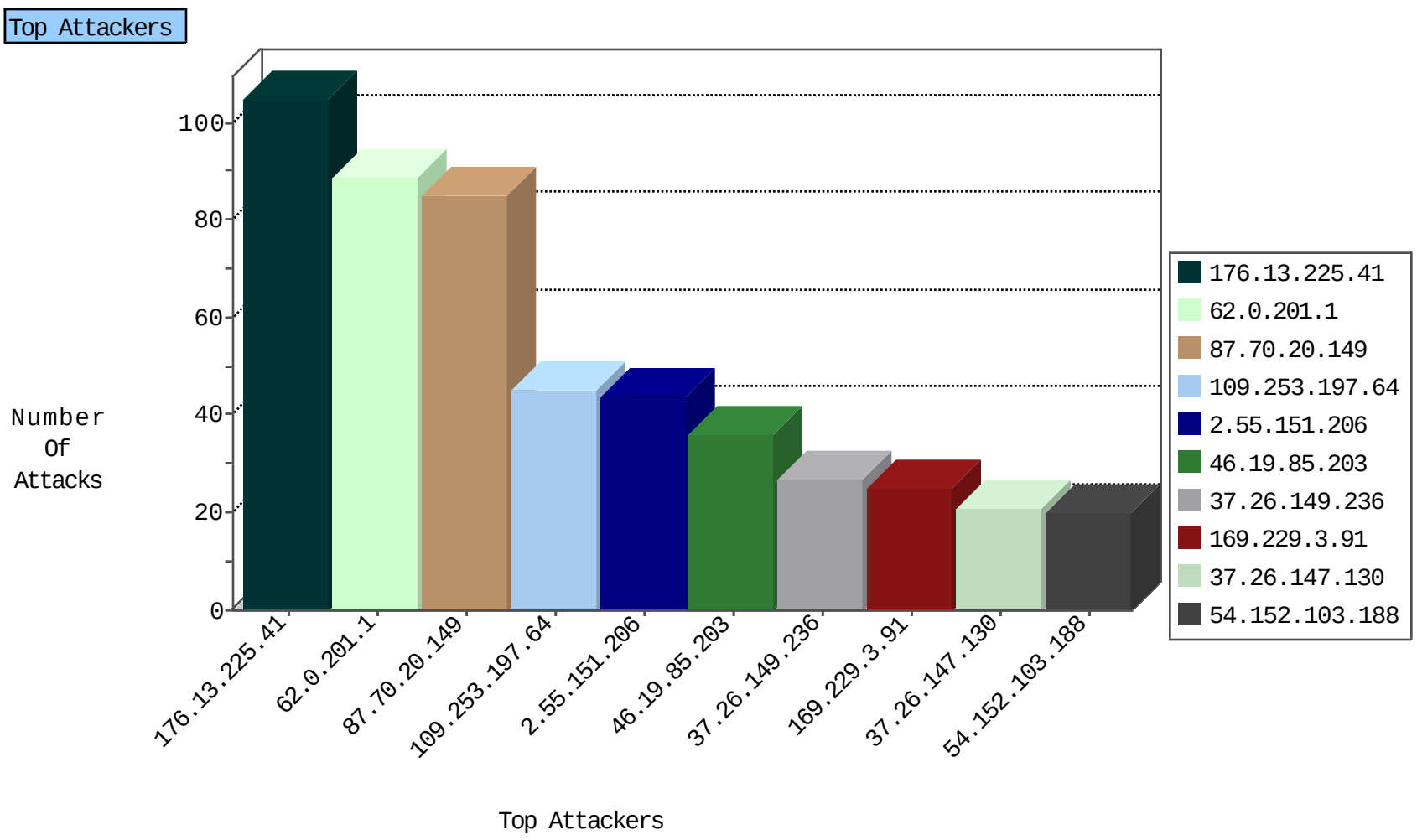
09-26-2016-15:04:07 to 09-26-2016-16:04:07

IDF Under Attack Daily Report





09-26-2016-15:04:07 to 09-26-2016-16:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.226.218	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
195.93.222.124	Poland	147.237.76.201	e.atal.idf.il	L4 Source or Dest Port Zero	drop	1

09-26-2016-15:04:07 to 09-26-2016-16:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.152.103.188	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	20
54.175.139.222	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	20
52.90.55.176	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	8

09-26-2016-15:04:07 to 09-26-2016-16:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.134.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.207.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.8.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.10.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.69	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
211.149.219.167	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.76.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.232.95.74	147.237.72.166	Georgia	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.61.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -f -sS	1
31.24.228.20	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.99.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.171.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.44.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.121.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.237.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.198.85	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.220.156.105	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.99.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.108.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.122.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 2048	1
31.24.228.20	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.63.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.179.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.82.238.67	147.237.8.46	Belgium	e.chinuch.idf.i	ET SCAN NMAP -sS window 3072	1

09-26-2016-15:04:07 to 09-26-2016-16:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.201.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	82
109.253.197.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
46.19.85.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.55.151.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
2.55.151.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
2.55.151.206	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.69.247.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.146.19	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.197.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
67.171.72.57	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.133.37	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
155.254.215.153	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
212.150.61.66	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
177.130.213.28	Brazil	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.132.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.92.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.106	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.201.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.197.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.197.64	Israel	147.237.77.216	dover.idf.il	SYN Attack		monitor	5
46.19.86.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.203.54	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
89.138.177.180	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
85.130.186.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.33	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.139.46.101	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
156.199.21.162	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.169	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
217.132.113.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.20.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-26-2016-15:04:07 to 09-26-2016-16:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.225.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
87.70.20.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
37.26.149.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.147.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.182.50	Block	18
109.253.142.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.242.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.120.156.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.164.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.187.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.161.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.196.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.129.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.79.42	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	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
31.168.125.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
76.100.149.61	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL ³ˇ„r•„<»~qÞÚƴ•'&˜ƒɔ•	Block	1
89.237.70.101	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.42	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	NULL Character in Method	Block	1
66.249.93.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
109.253.159.233	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
37.26.146.156	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.3.147.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.106.67	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.246.130.65	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	NULL Character in URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.65.50	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
207.232.18.46	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL ½ל7	Block	1
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/undefined	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	1
66.249.93.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
80.246.136.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1

09-26-2016-15:04:07 to 09-26-2016-16:04:07