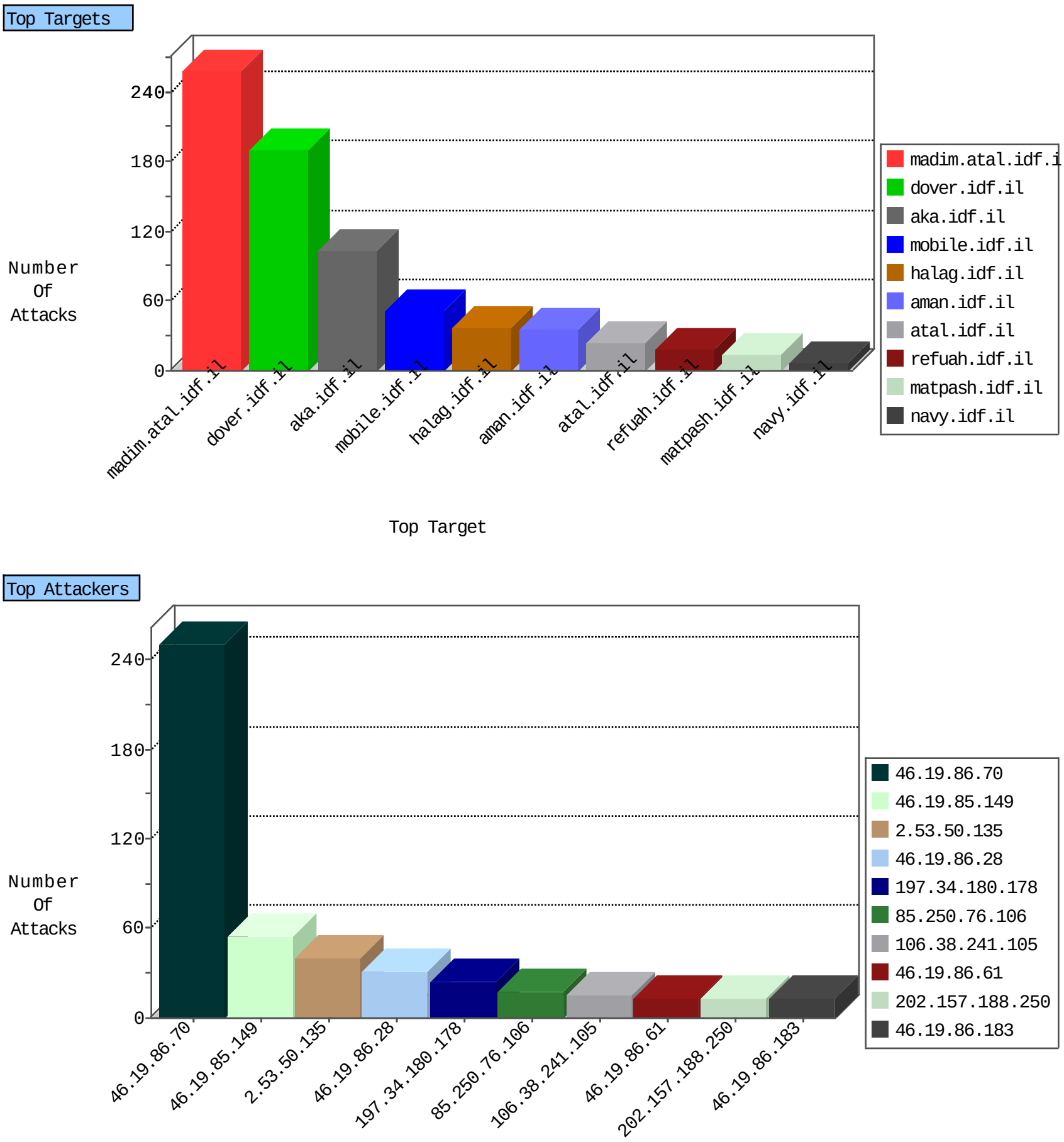
09-16-2016-18:04:06 to 09-16-2016-19:04:06

IDF Under Attack Daily Report



09-16-2016-18:04:06 to 09-16-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	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
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	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	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-18:04:06 to 09-16-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.241.212.165	United States	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-16-2016-18:04:06 to 09-16-2016-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
221.181.73.62	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.76.148	Indonesia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
116.72.137.42	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.69.129	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
221.181.73.62	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
116.72.137.42	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
116.72.137.42	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
103.207.39.82	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

09-16-2016-18:04:06 to 09-16-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.50.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
46.19.86.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
197.34.180.178	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
85.250.76.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.121.192.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.15.177	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.0.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.21.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
77.139.127.123	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.147.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
31.168.0.253	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.126	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.3.146	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.147.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.122	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
176.13.224.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
147.235.8.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.224.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
147.235.8.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.224.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
213.204.110.146	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.53.45.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
197.34.180.178	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.224.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.33.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
37.26.146.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.204.110.146	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.195	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.176.117.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
197.34.180.178	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.33.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-16-2016-18:04:06 to 09-16-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	251
46.121.192.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
2.53.50.135	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	3
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.67.179.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.59.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	2
46.19.86.205	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
202.157.188.250	Singapore	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 202.157.188.250	Block	1
109.253.228.131	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.33.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
202.157.188.250	Singapore	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 202.157.188.250	Block	1
31.33.234.159	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
176.13.250.55	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
89.248.172.16	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1474-he/refuah.aspx	Block	1
202.157.188.250	Singapore	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.86.205	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method a in URL	Block	1
140.147.236.195	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/giyus/general/	Block	1
79.177.113.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
202.157.188.250	Singapore	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.102.6.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
31.168.0.253	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
202.157.188.250	Singapore	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
93.173.55.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.115.145	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
202.157.188.250	Singapore	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 202.157.188.250	Block	1
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
79.180.4.146	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.102.8.215	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
202.157.188.250	Singapore	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 202.157.188.250	Block	1
202.157.188.250	Singapore	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
109.64.38.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
77.139.39.149	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
202.157.188.250	Singapore	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
46.116.45.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1515-en/dover.asp	Block	1
2.53.50.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.135.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
202.157.188.250	Singapore	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
202.157.188.250	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
202.157.188.250	Singapore	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/wp-login.php	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 159.220.74.2	Block	1
85.250.76.106	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/apple-app-site-association	Block	1
207.46.13.166	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in aka.idf.il/main/giyus/	None	1

09-16-2016-18:04:06 to 09-16-2016-19:04:06