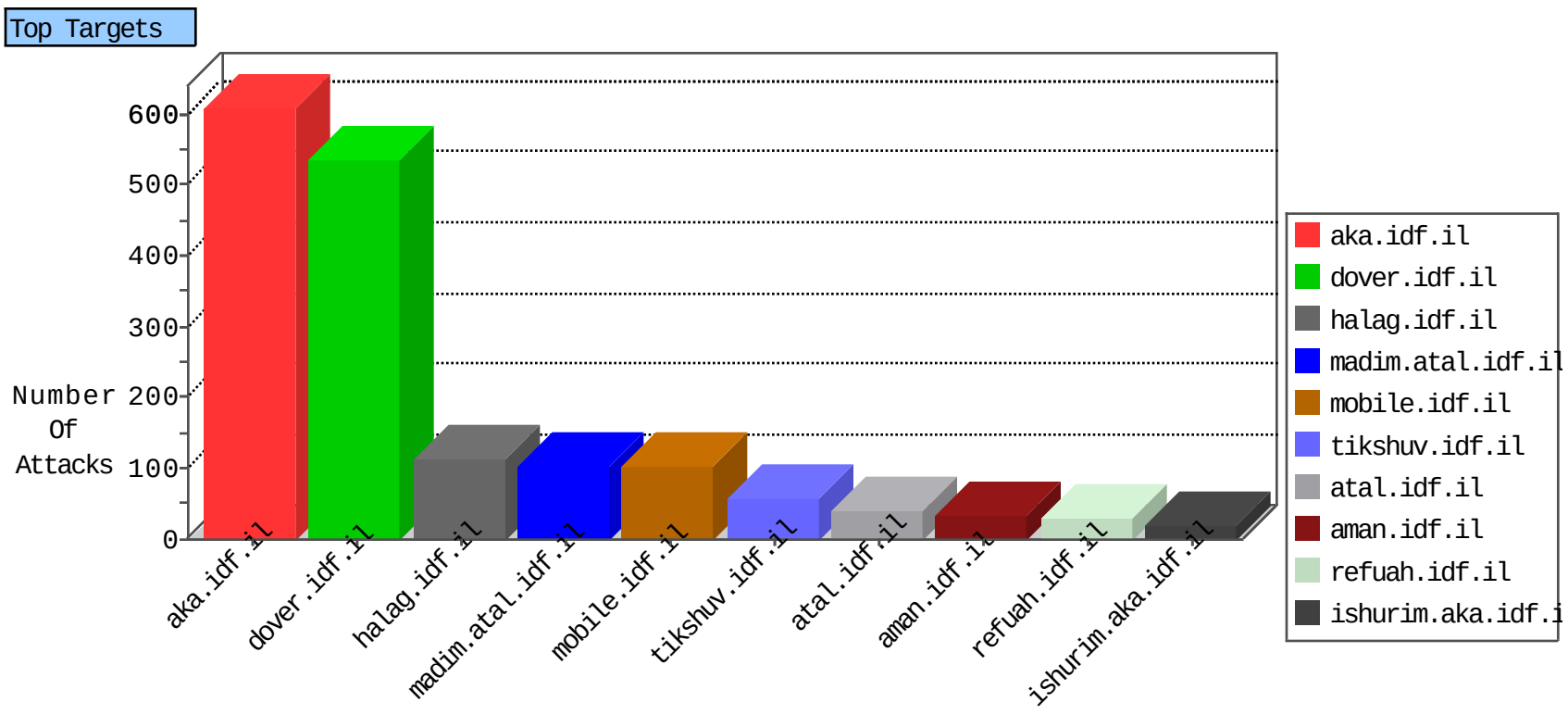
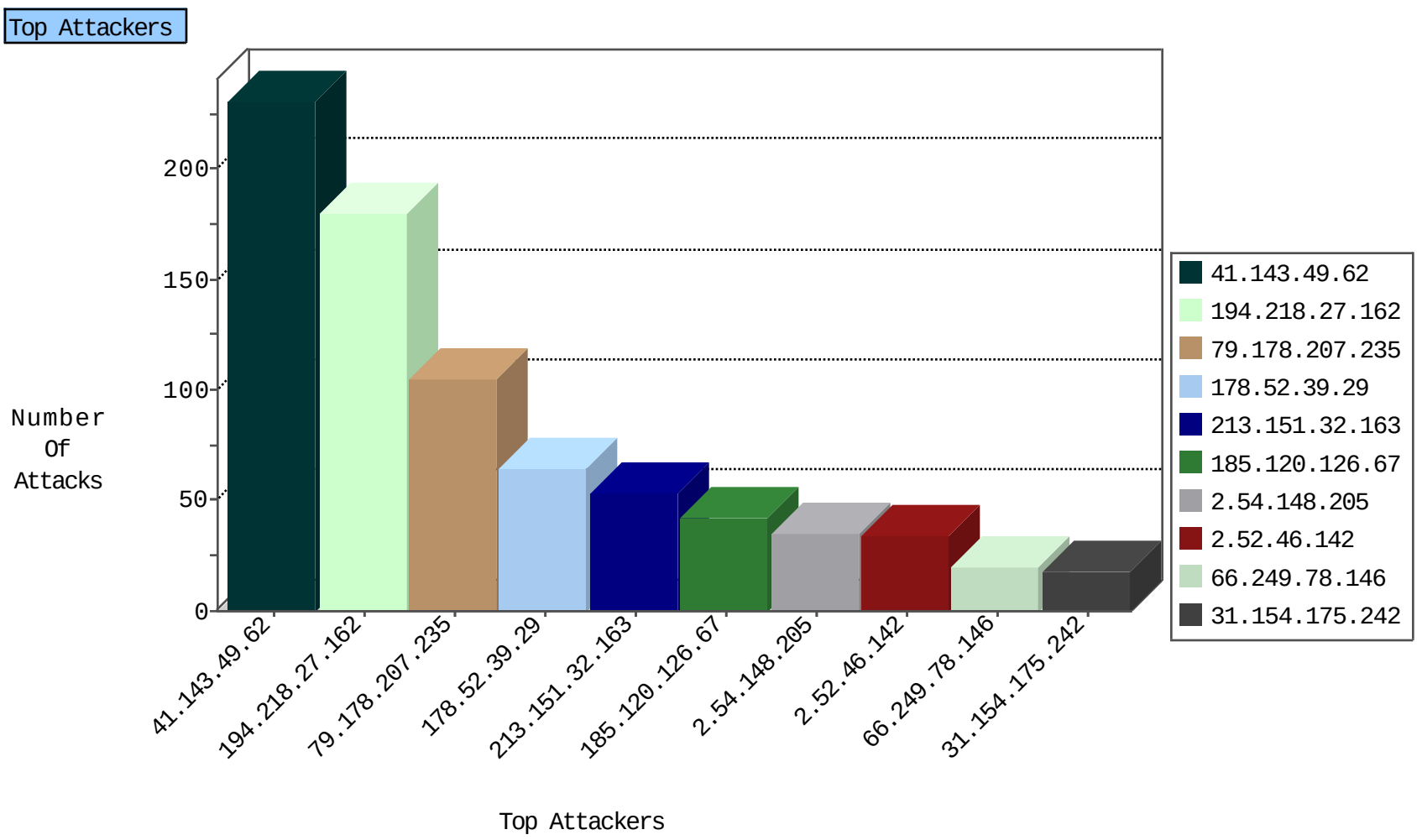
03-01-2016-19:04:00 to 03-01-2016-20:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-01-2016-19:04:00 to 03-01-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.143.49.62	Morocco	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1257
41.143.49.62	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	47
81.218.56.125	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.70	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
47.88.103.153	Canada	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
208.67.1.70	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
1.194.238.24	China	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1

03-01-2016-19:04:00 to 03-01-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.93.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
149.88.88.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.116.184.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
31.154.94.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
37.26.149.208	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.57.62.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.65.108.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.125.125.77	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.148	Italy	147.237.76.30	himush.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
168.235.155.26	Canada	147.237.76.42	refuah.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-01-2016-19:04:00 to 03-01-2016-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
168.235.155.26	147.237.76.42	Canada	refuah.idf.il	SERVER-WEBAPP admin.php access	1
40.113.118.99	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.85.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.100.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.131.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.169.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.6.23.67	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
203.212.101.2	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.173.36.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.76.39	India	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
89.133.67.3	147.237.0.35	Hungary	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
87.69.35.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.88.160.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
142.54.171.178	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
5.29.99.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.150.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.170.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
101.187.223.67	147.237.77.19	Australia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.174.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.76.39	India	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
89.139.166.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
89.133.67.3	147.237.0.35	Hungary	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
192.116.159.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.44.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-19:04:00 to 03-01-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
79.178.207.235	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
178.52.39.29	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
178.52.39.29	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
77.127.204.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.120.126.67		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
5.22.131.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
89.138.122.232	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.253.215.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.22.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.138.99.166	Martinique	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
185.120.126.67		147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
2.52.46.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.17.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.46.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.6.226	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.228.185.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.46.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.144.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.117.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.46.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.234.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.154.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.46.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.253.147.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.236.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.109.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.176.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.181.101	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.138.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.105.28	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.3	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.108.108.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
94.188.146.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.92	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.3	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.108.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.188.146.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.120.126.67		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.108.108.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.54.148.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
31.154.175.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.175.242	Block	11
66.249.84.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
37.120.23.171	Germany	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 37.120.23.171	Block	7
31.154.175.242	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
66.249.84.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	5
79.178.148.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	4
66.249.66.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.84.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.120.23.171	Germany	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	4
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.60.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
170.74.231.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	3
176.13.5.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.89.217.224		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.28.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
168.235.155.26	Canada	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
109.253.215.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.86.97.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyos	Block	2
176.13.12.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.89.217.230		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.94.69	Block	2
85.250.242.115	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.242.115	Block	2
79.182.12.10	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
73.157.173.70	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.168.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
109.65.93.122	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.138.122.232	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.108.237.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.121.82.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
37.26.148.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.113.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/images/tofes106/	Block	1
5.166.204.26	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
212.66.40.76	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.97.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
149.88.141.151	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.141.151	Block	1
79.182.146.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
73.224.78.156	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.168.56	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1