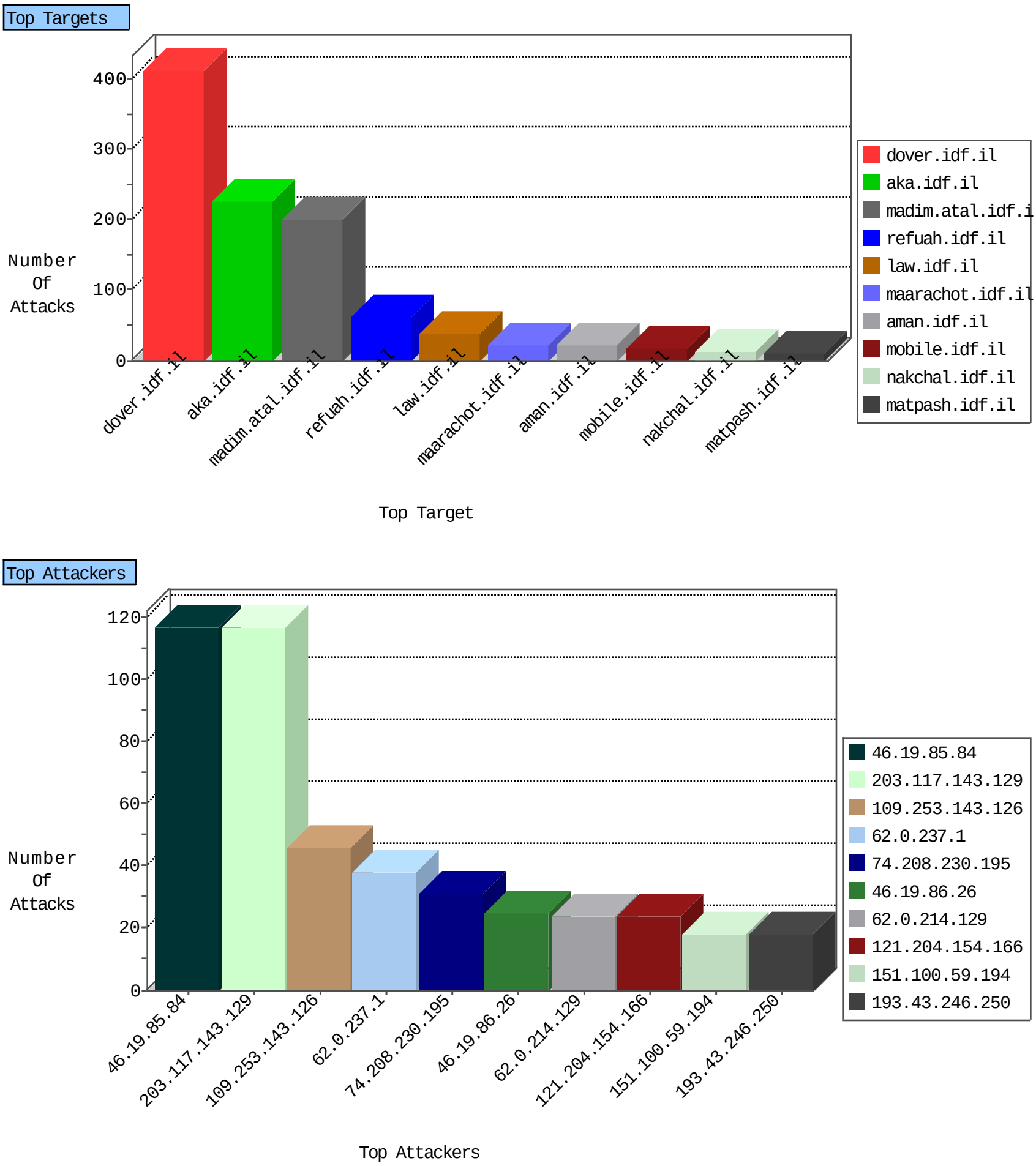
09-13-2016-11:04:02 to 09-13-2016-12:04:02

IDF Under Attack Daily Report



09-13-2016-11:04:02 to 09-13-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.100.59.194	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	18
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	9
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
141.22.213.35	Germany	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	5
176.13.244.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
203.117.143.129	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
129.22.150.78	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.69	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
120.132.50.135	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
200.19.159.35	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
170.140.119.70	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-11:04:02 to 09-13-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-13-2016-11:04:02 to 09-13-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	25
79.182.32.127	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
168.235.197.242	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.106.162.152	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.68.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.152.94.130	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.139.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.242.74.253	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
220.242.82.131	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
80.179.96.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.83.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.22.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.245.173.142	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
132.68.64.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.130.115	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
111.23.12.94	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
31.210.186.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.157.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.61.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.168	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
220.242.82.131	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
82.81.214.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.83.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.61.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.66.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.32.127	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
172.245.173.142	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-13-2016-11:04:02 to 09-13-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
203.117.143.129	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.220.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
84.208.199.45	Norway	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
2.53.61.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.204.33	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.233	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
62.0.209.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.244.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.14.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.132.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.238.59	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.22.229	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.243	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.243	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.233.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
118.70.16.65	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
95.35.152.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.204.33	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.22.229	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
81.218.116.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
81.218.116.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
59.147.202.158	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.103	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.247.168	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.109.214.179	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
217.194.203.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.61.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-13-2016-11:04:02 to 09-13-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
109.253.143.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
121.204.154.166	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.204.154.166	Block	17
80.246.138.162	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	12
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.244.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
121.204.154.166	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
195.160.242.40	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	5
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.7.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.197.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.24.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
2.55.39.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.114.38.126	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
77.138.244.237	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
195.160.242.40	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	2
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.11.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.114.38.126	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.114.38.126	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	2
46.19.85.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
147.236.238.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.19.85.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
141.0.15.159	Norway	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
121.204.154.166	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
2.55.22.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.245.1	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
147.236.238.20	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
213.8.163.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.139.110.200	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
132.74.7.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
82.166.83.74	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
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.66.161	Block	1
217.194.203.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.220.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.35.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
141.0.14.74	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/home/default.asp	Block	1
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
109.197.22.206	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.197.22.206	Block	1
66.249.93.91	Israel	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/../../images/shared/sub_menu_bottom.png	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
79.182.32.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/main	Block	1
195.27.53.211	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
185.32.179.174	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	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

09-13-2016-11:04:02 to 09-13-2016-12:04:02