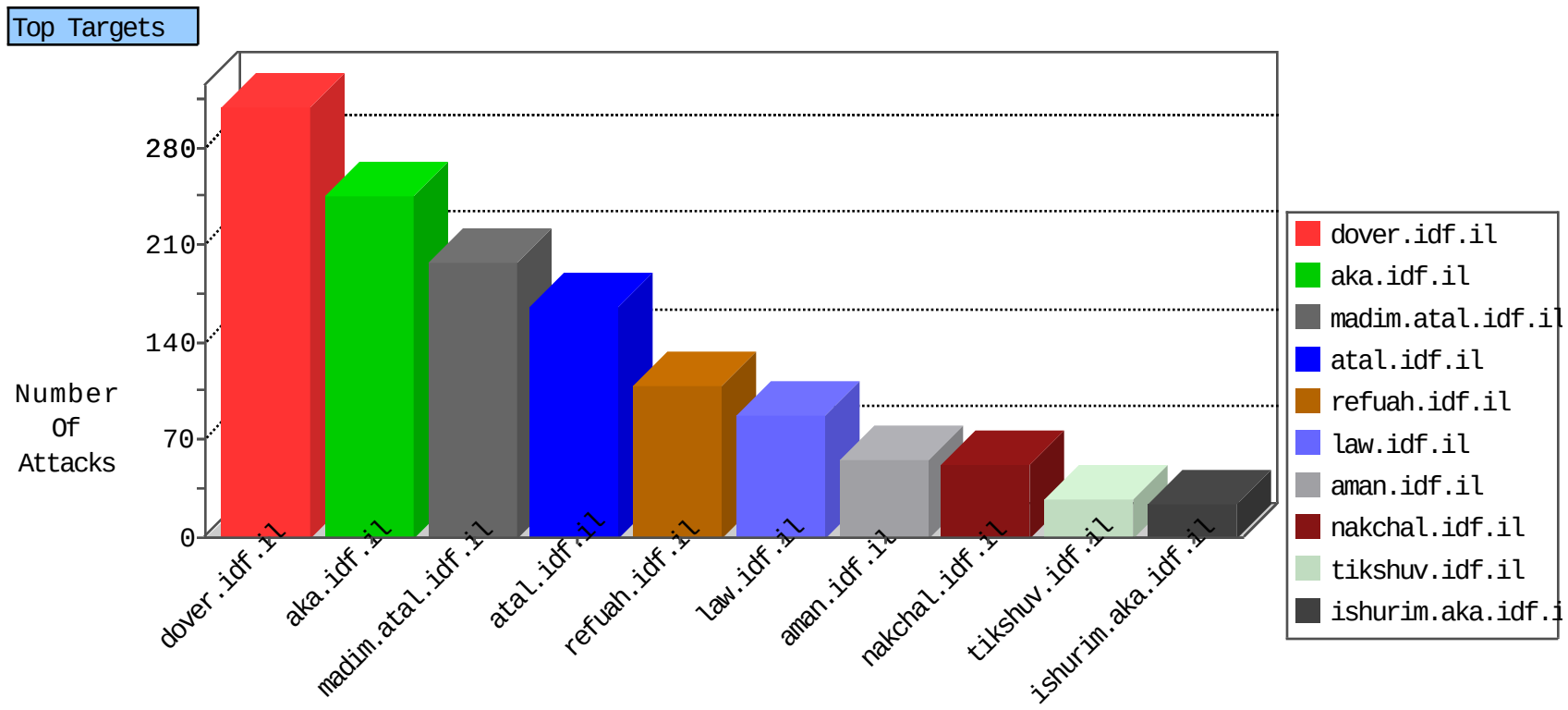
09-12-2016-10:04:02 to 09-12-2016-11:04:02

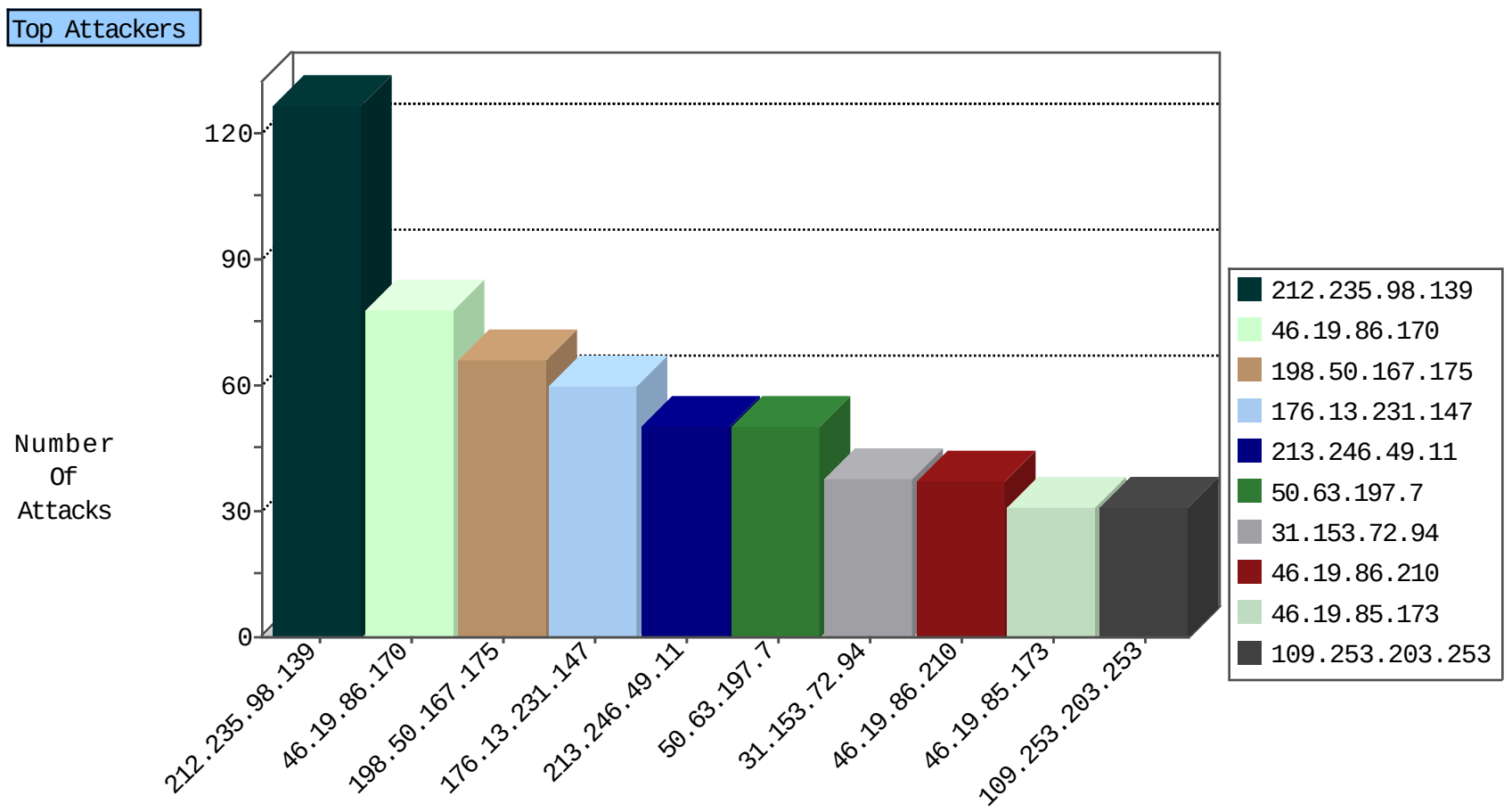
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-12-2016-10:04:02 to 09-12-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.23.215	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
212.179.64.162	Israel	147.237.72.156	aman.idf.il	Black List	drop	3
2.53.43.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
46.19.85.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.68	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
79.179.215.176	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
134.197.113.3	United States	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

09-12-2016-10:04:02 to 09-12-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	30
50.63.197.7	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.46.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.11	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.7	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.80	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.109.70	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
213.246.49.11	France	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
46.236.115.84	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.11	France	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
213.246.49.11	France	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	3
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
50.63.197.11	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
187.17.109.70	Brazil	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-12-2016-10:04:02 to 09-12-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.63.197.7	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	32
213.246.49.11	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	32
177.185.194.80	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	15
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
187.17.109.70	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	14
184.168.46.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
46.236.115.84	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	14
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	12
50.63.197.11	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
46.254.9.91	147.237.76.199	Sweden	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
103.255.47.41	147.237.8.45	Hong Kong	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
39.120.12.204	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.159.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.39.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	1
62.219.153.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.10.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.68.115.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.158.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.249.197	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.228.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.195.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.23.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.52.71	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.204.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.177.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.135.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.102.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
132.73.202.85	147.237.77.216	Israel	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
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.27.142.85	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.203.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-12-2016-10:04:02 to 09-12-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	97
31.153.72.94	Cyprus	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	34
109.253.203.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
109.253.228.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
107.167.112.194	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
82.166.198.101	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
84.229.75.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
212.29.223.233	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
2.55.3.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
117.229.98.104	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.129.122.98	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.225.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.145.120	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.96.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.198	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.197	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.225.254	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.81.67.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
141.226.217.160	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.81.67.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.99	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
198.50.167.175	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.201.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.134.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
198.50.167.175	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.29.223.233	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
198.50.167.175	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
198.50.167.175	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.135	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.153.72.94	Cyprus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.231.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.161.239	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
185.32.179.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.229	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
109.253.219.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.137.9.90	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
37.26.147.128	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.58.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.228.133.208	Cyprus	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.246.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
10.152.70.33		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
82.166.83.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
37.26.149.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.52.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.138.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.203	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method er.aspx in URL	Block	1
156.167.205.109	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
82.166.114.235	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.139.161.239	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.161.239	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.233.228	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
95.86.104.181	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
37.26.147.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
156.167.205.109	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.229.75.137	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
95.253.205.134	Italy	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
2.53.144.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.121.154	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
37.26.148.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
156.167.205.109	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/index.php	Block	1
79.180.92.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
192.116.177.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
2.55.21.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.140.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.129.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
37.26.148.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.17.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.228.133.208	Cyprus	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
212.29.223.233	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.86.203	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1

09-12-2016-10:04:02 to 09-12-2016-11:04:02