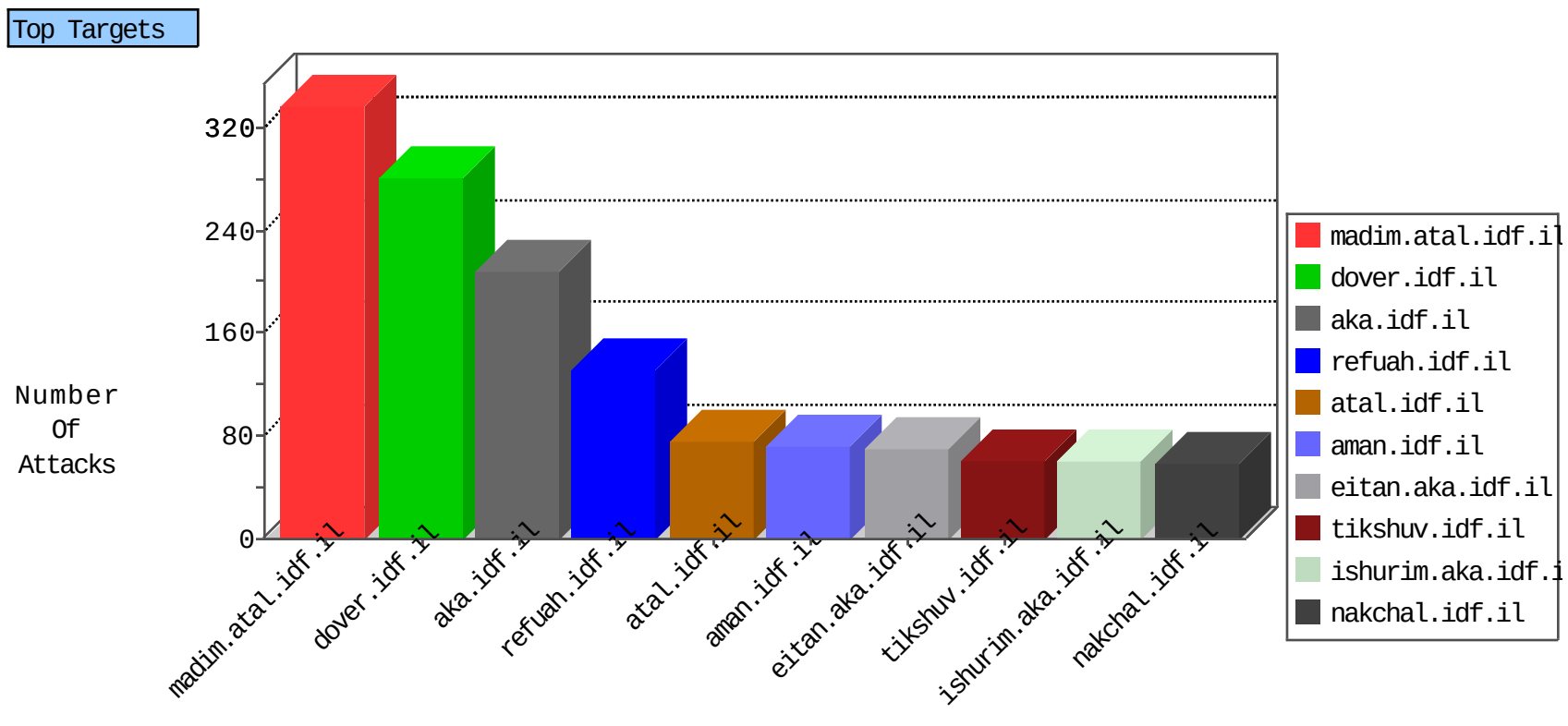
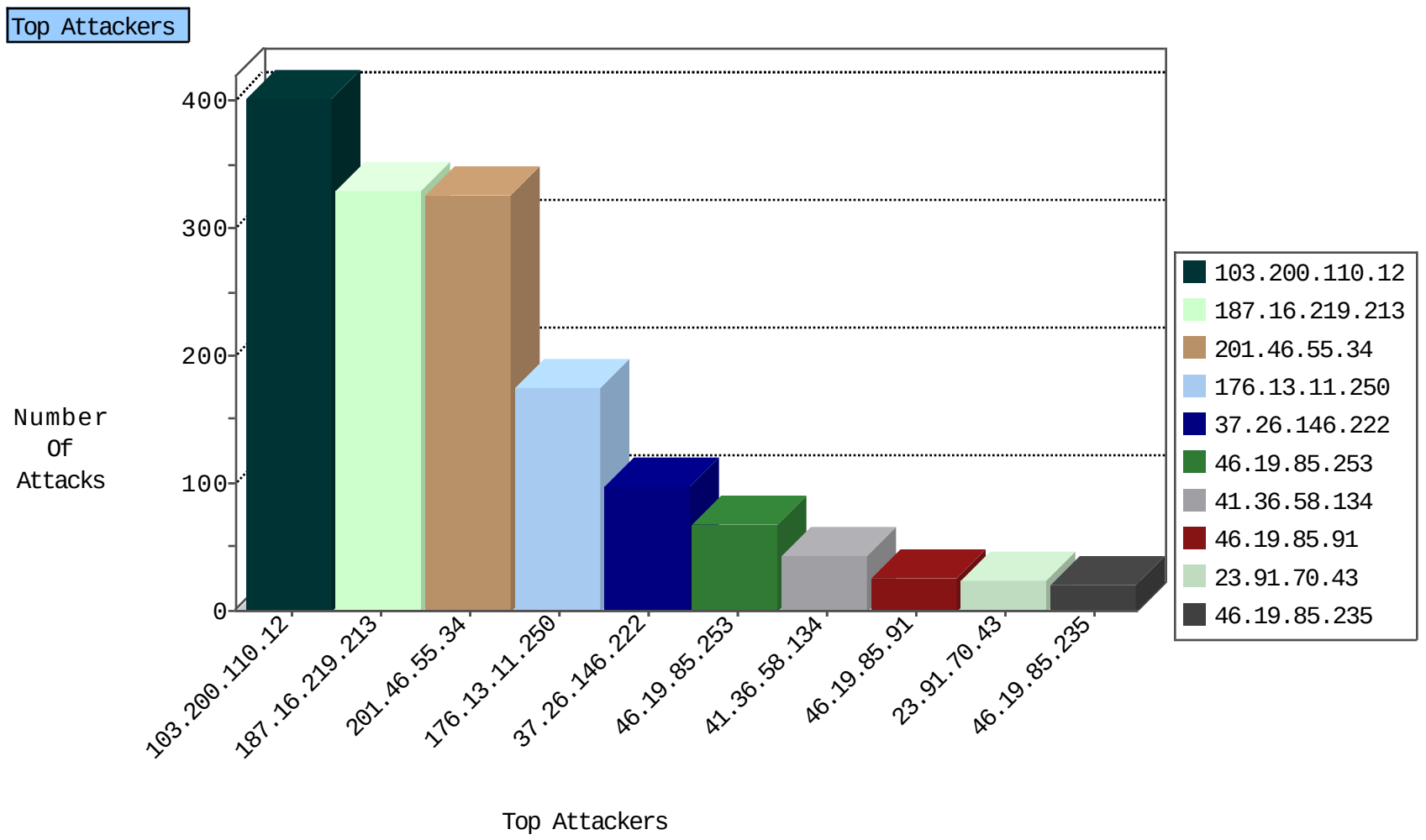
09-12-2016-23:04:04 to 09-13-2016-00:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-12-2016-23:04:04 to 09-13-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
2.53.147.45	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	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
129.32.84.160	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
104.243.16.128	United States	147.237.8.50	e.tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
121.199.18.160	China	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	1
216.48.80.14	Canada	147.237.72.156	aman.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
204.85.191.10	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
219.141.189.72	China	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
192.33.90.68	Switzerland	147.237.72.217	e.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
103.16.199.144	Indonesia	147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	1

09-12-2016-23:04:04 to 09-13-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.91.70.43	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
213.252.247.231	Lithuania	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-12-2016-23:04:04 to 09-13-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.43	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
176.9.124.208	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	12
176.9.124.208	147.237.77.216	Germany	dover.idf.il	LOCAL_RULES access attempt to file_manager.php	2
94.183.161.18	147.237.72.166	Iran, Islamic Republic of	aka.idf.il	ET SCAN Potential SSH Scan	1
104.243.16.128	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.128	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
52.166.249.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.128	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
94.183.161.18	147.237.77.234	Iran, Islamic Republic of	halag.idf.il	ET SCAN Potential SSH Scan	1
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
94.183.161.18	147.237.77.19	Iran, Islamic Republic of	law-forum.idf.il	ET SCAN Potential SSH Scan	1
40.86.75.227	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.183.161.18	147.237.76.176	Iran, Islamic Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
200.111.107.58	147.237.77.178	Chile	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.183.161.18	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.183.161.18	147.237.72.167	Iran, Islamic Republic of	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.243.16.128	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.128	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.168	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.128	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
52.166.130.115	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
104.243.16.128	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.117.223.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.183.161.18	147.237.77.178	Iran, Islamic Republic of	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
41.36.58.134	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
94.183.161.18	147.237.76.199	Iran, Islamic Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.86.75.227	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.183.161.18	147.237.76.148	Iran, Islamic Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.149	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.183.161.18	147.237.72.217	Iran, Islamic Republic of	e.idf.il	ET SCAN Potential SSH Scan	1

09-12-2016-23:04:04 to 09-13-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
46.19.85.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
103.200.110.12	Hong Kong	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
103.200.110.12	Hong Kong	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
184.168.192.134	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
103.200.110.12	Hong Kong	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
103.200.110.12	Hong Kong	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
103.200.110.12	Hong Kong	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
187.16.219.213	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.16.219.213	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
85.64.94.187	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
187.16.219.213	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.16.219.213	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.16.219.213	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15

09-12-2016-23:04:04 to 09-13-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.11.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	175
37.26.146.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
95.86.85.15	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.85.15	Block	6
176.13.244.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
83.6.57.248	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	4
2.53.131.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.86.85.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/69693.jpg	Block	2
79.181.188.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.160.105	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/exampcert	Block	1
46.19.85.229	Israel	147.237.77.176	matpash.idf.il	Malformed URL com.android.browser	Block	1
137.200.32.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
80.241.214.29	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3469.jpg	Block	1
31.168.0.253	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/printpreview/default.asp	Block	1
77.138.241.83	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
207.241.229.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/404.aspx	Block	1
46.19.85.229	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method X-Requested-With: in URL com.android.browser	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
77.139.175.211	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
209.171.43.251	Canada	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
176.13.233.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=73556	Block	1
46.19.85.229	Israel	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
109.66.149.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
213.57.79.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	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
2.53.131.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.215.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.240	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
46.19.85.229	Israel	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
79.181.188.212	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.139.219.209	Spain	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.26	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
89.139.218.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-12-2016-23:04:04 to 09-13-2016-00:04:04