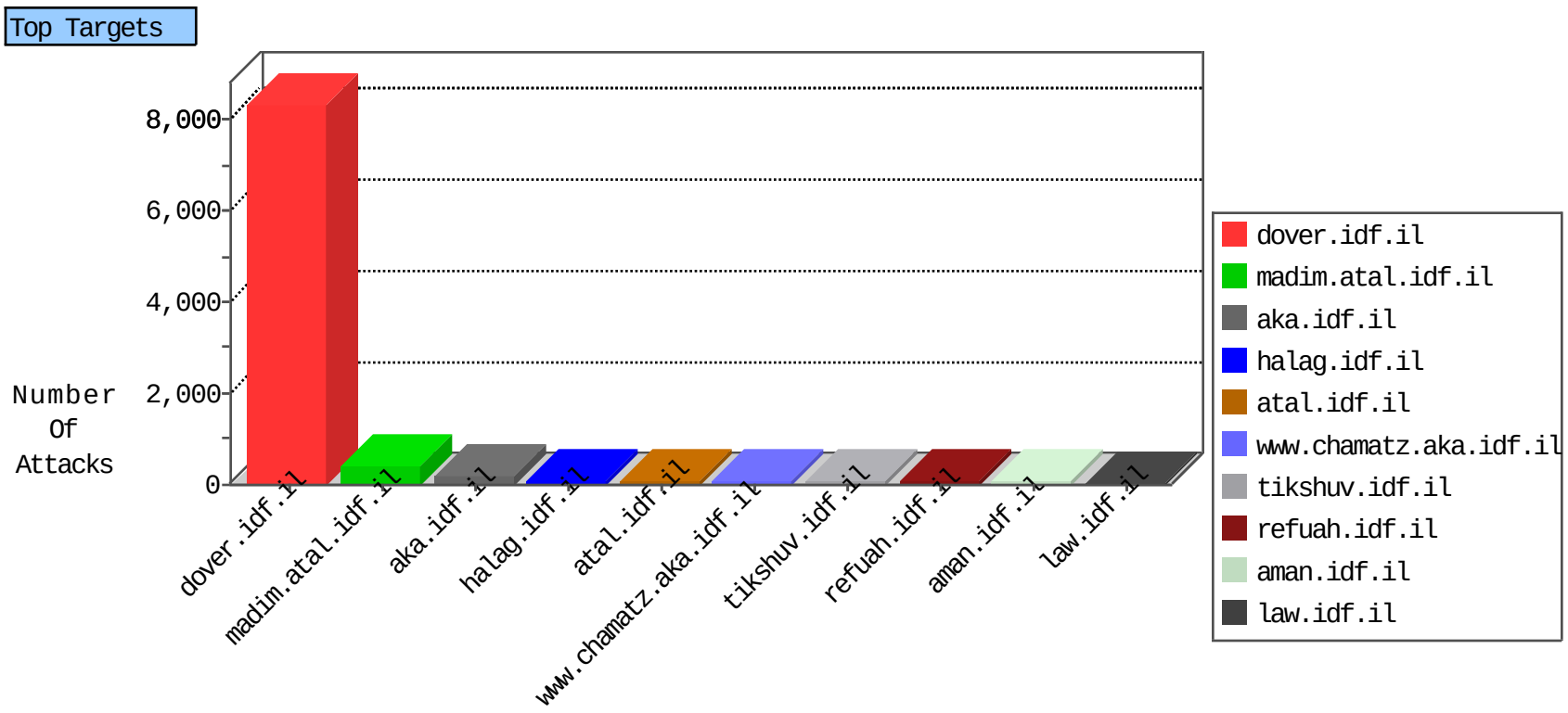
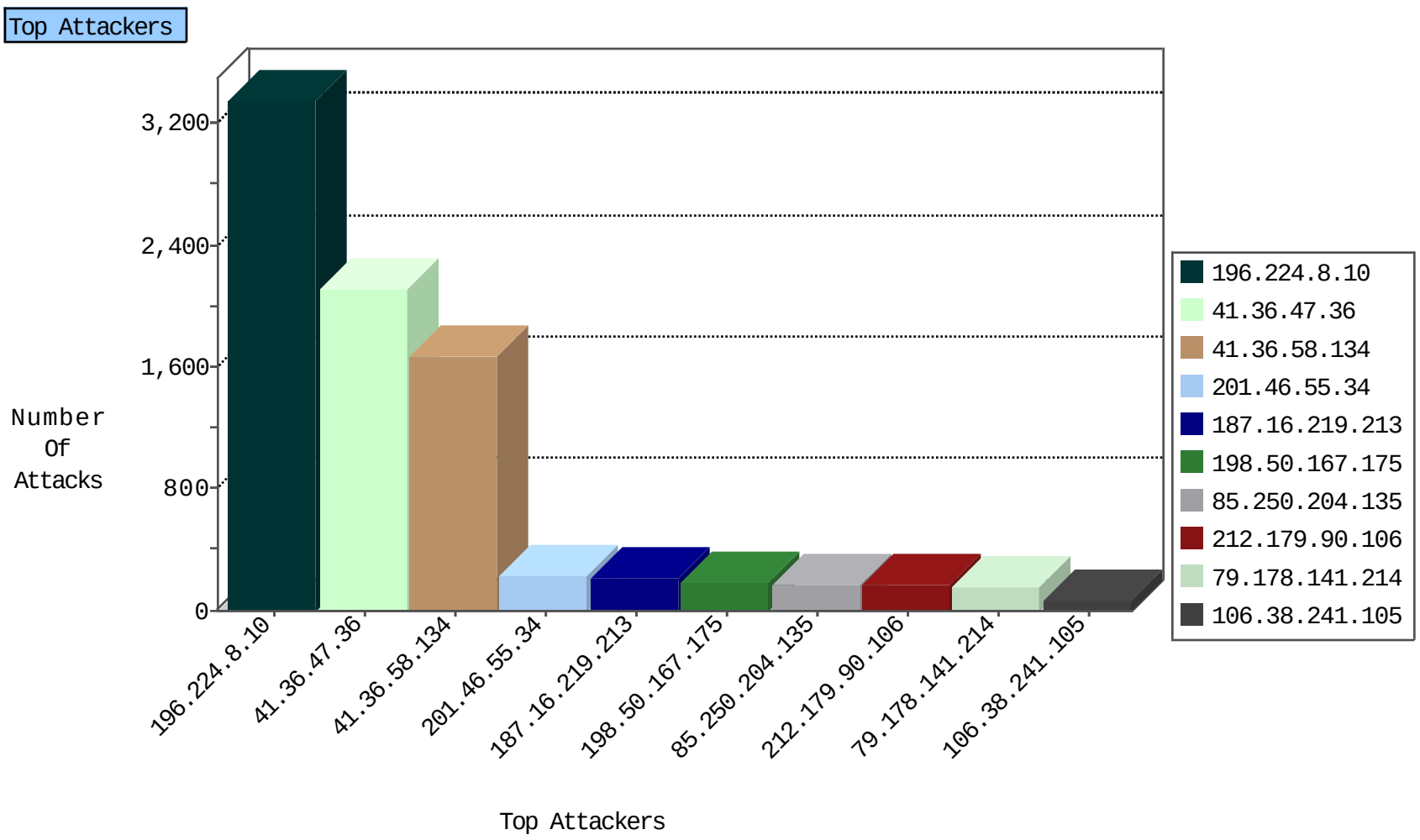
09-12-2016-20:04:08 to 09-12-2016-21:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-12-2016-20:04:08 to 09-12-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.36.47.36	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
190.210.74.49	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
128.223.8.112	United States	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
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	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	1
85.65.196.178	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	1
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	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
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
85.65.196.178	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
111.73.45.159	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
77.124.59.223	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
125.75.206.183	China	147.237.8.45	e.eitan.idf.il	Invalid TCP Flags	drop	1

09-12-2016-20:04:08 to 09-12-2016-21:04:08

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	7
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
197.118.191.15	Algeria	147.237.0.34	tikshuv.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-12-2016-20:04:08 to 09-12-2016-21:04:08

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
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
45.79.71.122	147.237.77.74	United States	law.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.0.236.165	147.237.77.178	Moldova, Republic of	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
40.86.75.227	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.17.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.234	Pakistan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.179	Pakistan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.194.148	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.149	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.235	Netherlands	sviva.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
188.0.236.165	147.237.77.243	Moldova, Republic of	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
40.86.75.227	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.235	Pakistan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.216	Pakistan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-12-2016-20:04:08 to 09-12-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.224.8.10	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3348
41.36.47.36	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2104
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1662
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	162
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
84.95.60.218	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	36
116.0.250.57	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
109.253.134.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.23	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.102.8.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
77.139.96.71	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.102.8.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
176.13.239.23	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
80.246.130.62	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
5.28.190.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.8.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
89.138.167.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.36	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
82.80.159.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.238.156.18	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
187.16.219.213	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
77.138.183.135	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
2.53.166.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
79.178.193.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
68.180.229.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
213.8.204.8	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.80	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
201.46.55.34	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.86.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11

09-12-2016-20:04:08 to 09-12-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.204.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
79.178.141.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
213.8.204.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.67.185.219	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
5.29.118.55	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.80	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
109.67.49.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.51.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.193.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
37.26.146.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
176.58.69.207	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.58.69.207	Block	1
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
2.53.52.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.220.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/bamahane	Block	1
109.253.215.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.238.156.18	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	1
87.69.109.125	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	Block	1
69.31.50.56	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
46.19.85.84	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method f450ej0pceygxwxnm45 in URL	Block	1
176.58.69.207	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin	Block	1
109.67.185.219	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.67.185.219	Block	1
80.246.130.62	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
46.19.85.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.69.109.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
69.115.134.82	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1038-en/dover.aspx parameter ctl00$ContentPlaceHolder1$txtEmail	Block	1
46.19.86.36	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.169.7.223	United States	147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
5.29.119.159	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1197-he/refuah.	Block	1
109.67.185.219	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
84.111.216.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteyerua	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
157.55.39.254	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/kishur/default.asp	None	1
89.139.136.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl61 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
70.211.20.104	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/mesiratmeida	Block	1
109.253.132.105	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
31.210.186.176	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/exampcert/	Block	1
85.64.7.96	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.13	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/talking_from_field/	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1

09-12-2016-20:04:08 to 09-12-2016-21:04:08