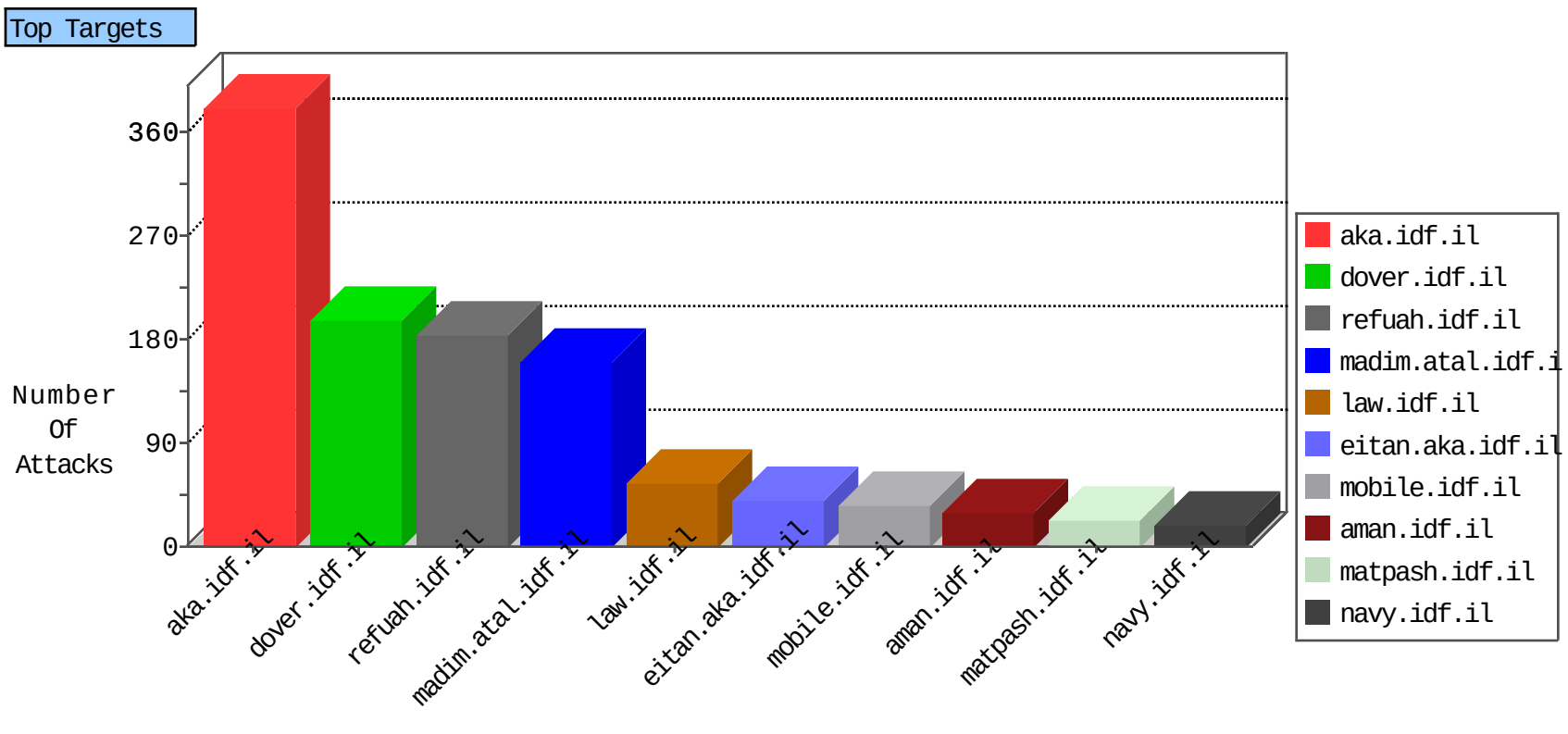
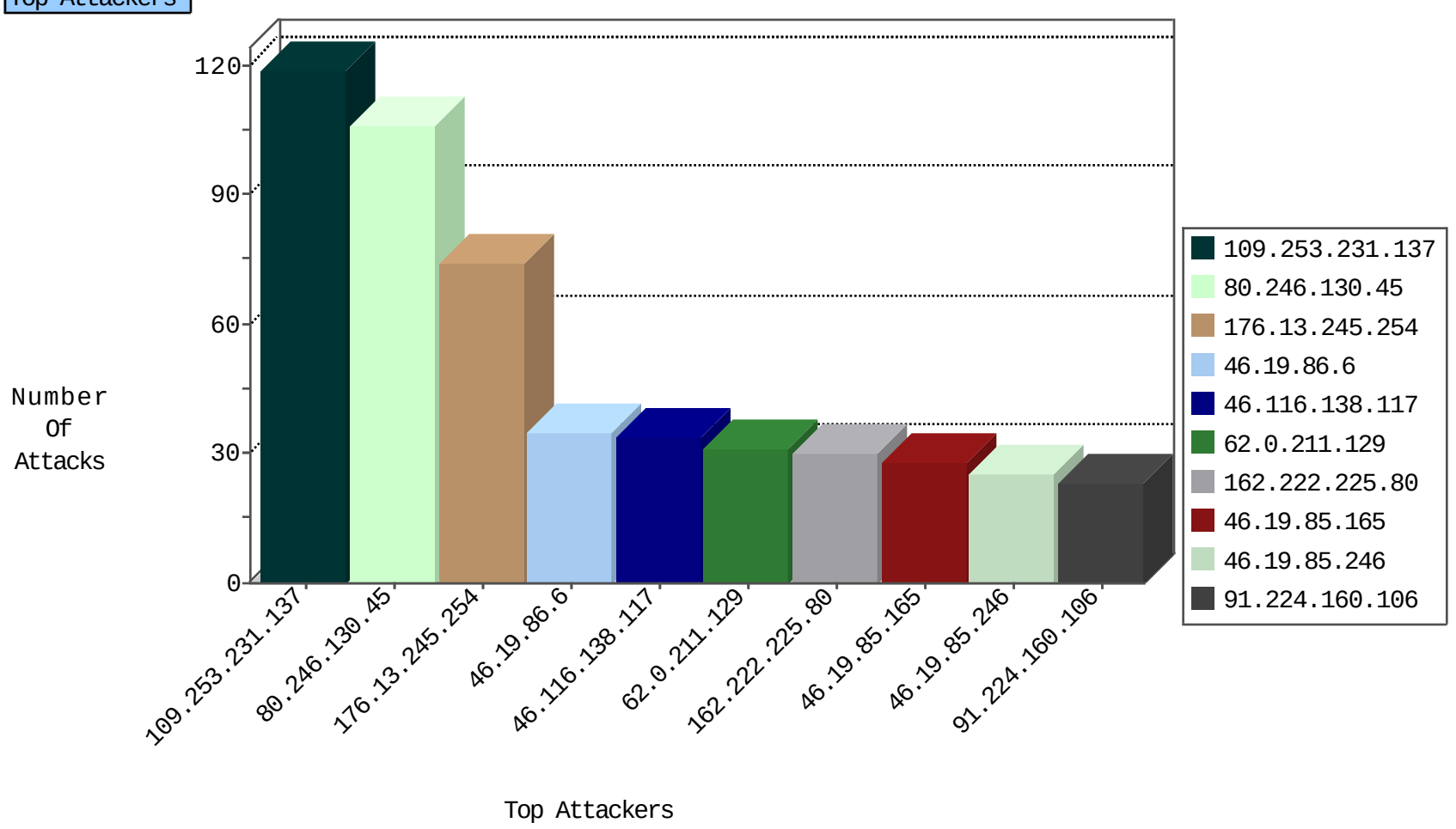
09-14-2016-14:04:08 to 09-14-2016-15:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-14-2016-14:04:08 to 09-14-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.91.224.79	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	956
132.66.62.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	236
79.182.63.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	38
109.67.240.132	Israel	147.237.72.166	aka.idf.il	Black List	drop	20
37.26.147.149	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
199.203.151.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
81.218.136.51	Israel	147.237.77.216	dover.idf.il	Black List	drop	5
79.180.189.163	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
109.65.183.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
141.212.113.178	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.179	e.mazi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
69.30.193.253	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
81.218.136.51	Israel	147.237.76.31	nakchal.idf.il	Black List	drop	1
164.107.127.12	United States	147.237.72.166	aka.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
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.118	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
91.224.160.106	Netherlands	147.237.77.176	matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
69.30.193.251	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
192.116.94.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
81.218.118.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-14-2016-14:04:08 to 09-14-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.222.225.80	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-14-2016-14:04:08 to 09-14-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.222.225.80	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	24
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
121.46.100.208	147.237.77.74	India	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.188.162.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
212.227.55.94	147.237.77.212	Germany	e.dover.idf.il	ET SCAN Potential SSH Scan	1
87.203.120.42	147.237.77.216	Greece	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
212.25.73.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.191.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.6.97	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.151.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.116.66.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
2.55.188.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.52.236.242	147.237.76.42	Thailand	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
2.53.162.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.67.178.150	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
213.8.121.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.86.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
78.39.133.4	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
203.171.187.8	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.219.110.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.34.57.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.16.142.100	147.237.77.216	Cyprus	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
2.53.175.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.14.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-14-2016-14:04:08 to 09-14-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
46.116.138.117	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
62.0.211.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.245.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
176.13.245.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
46.19.85.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
176.13.245.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
62.0.212.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.245.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
2.55.29.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
176.13.245.254	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	11
46.19.86.6	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
100.92.28.230		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
213.57.70.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.6	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.57.70.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.6	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
2.53.61.252	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.231.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.15.27	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.137.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
62.0.200.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.24.207.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.90.49.25	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.229	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
194.90.25.122	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.168.92.42	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.240.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
181.124.104.128	Paraguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.231.137	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.147.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.204.39	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
100.92.28.230		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

09-14-2016-14:04:08 to 09-14-2016-15:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.231.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.67.178.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	Block	8
77.138.6.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	7
46.19.85.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
195.60.235.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.60.235.57	Block	4
109.67.178.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.178.150	Block	4
80.246.139.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	4
37.26.148.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.230.222	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
37.26.147.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.178.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/	Block	2
79.178.181.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
77.139.230.222	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.117.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.84.103	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.1.120	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.55.1.120	Block	2
109.253.134.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	2
80.246.140.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
62.219.132.57	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
104.236.220.154	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
195.60.235.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter nfr in www.aka.idf.il/sip_storage/files/6/68516.gif	None	1
80.179.37.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
77.139.230.222	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
45.55.229.109	United States	147.237.77.176	matpash.idf.il	Unauthorized Method HEAD for 147.237.77.176/	Block	1
66.249.76.77	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/mobile/templates/getfile/getfile.aspx	Block	1
2.55.29.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.118.91.163	Ukraine	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
185.46.214.76	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.165	Israel	147.237.77.233	atal.idf.il	Malformed URL	Block	1
109.253.158.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.139.190.227	France	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.157	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
212.25.84.200	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
80.246.130.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
176.13.21.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-14-2016-14:04:08 to 09-14-2016-15:04:08