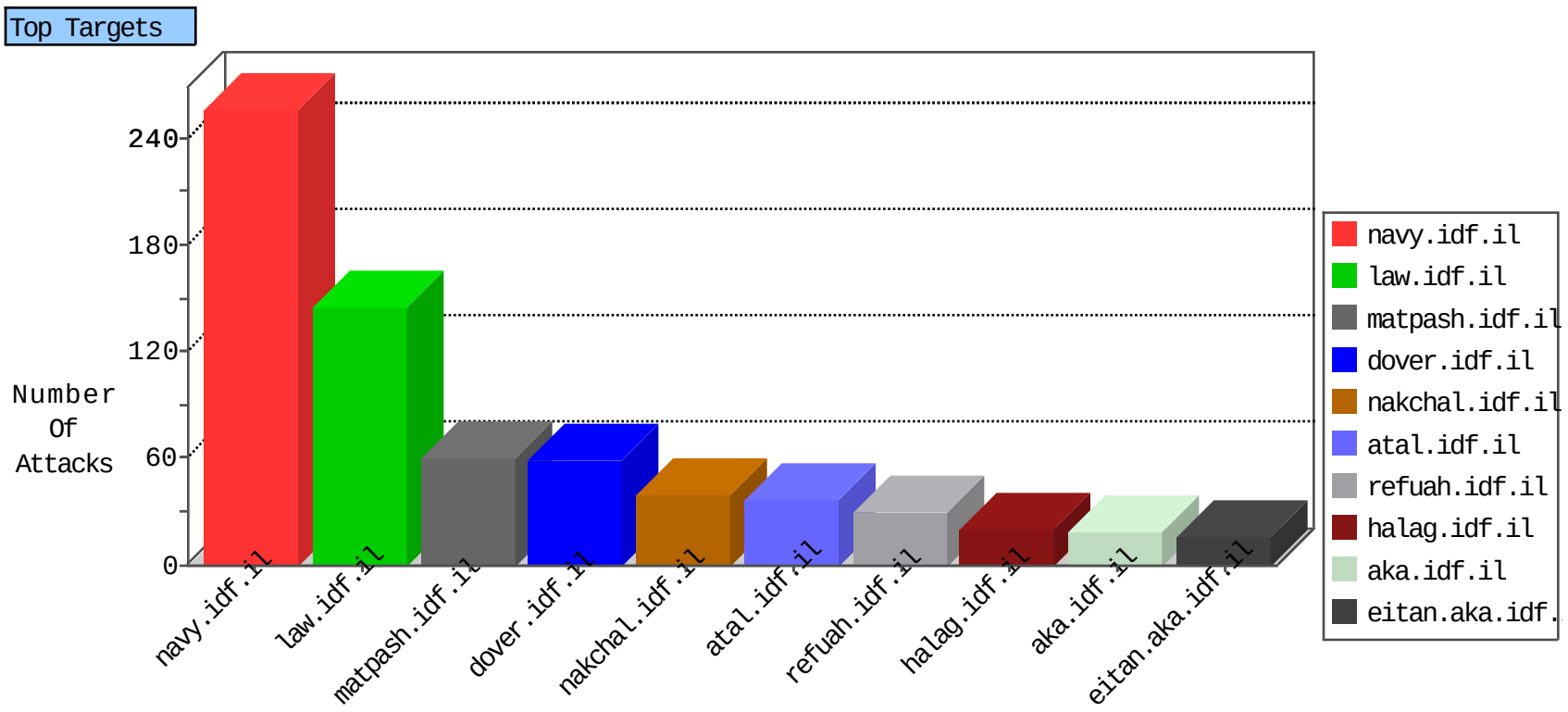
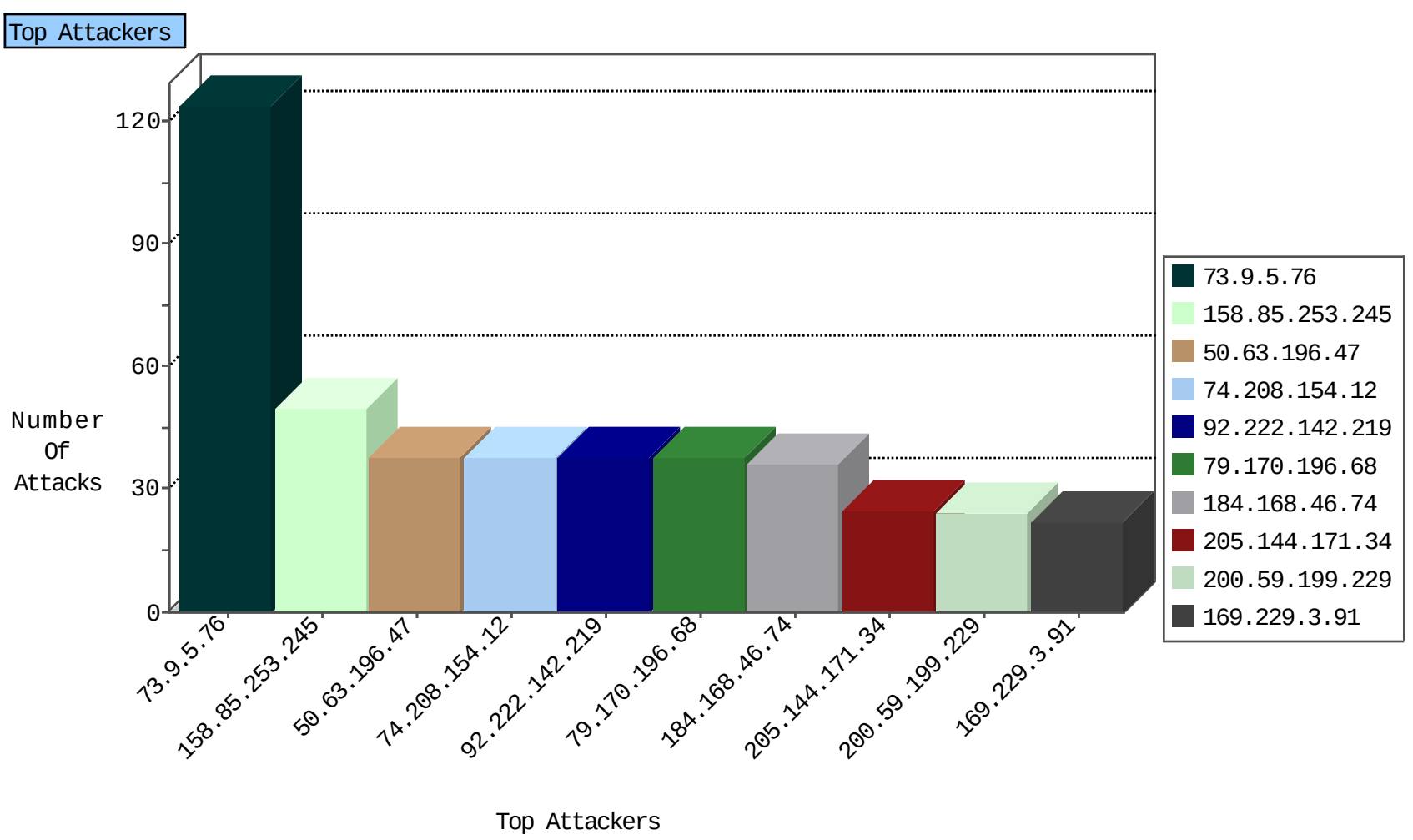
09-22-2016-01:10:07 to 09-22-2016-02:10:07

IDF Under Attack Daily Report





09-22-2016-01:10:07 to 09-22-2016-02:10:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.231.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
173.208.197.205	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
63.141.242.197	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
69.30.193.253	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.197.203	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.226.222	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
142.54.174.84	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
63.141.231.197	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
204.12.220.86	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
142.54.174.84	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
69.30.226.218	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
185.81.157.152	France	147.237.76.34	yohalan.idf.il	Black List	drop	1
87.112.221.124	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
173.208.150.117	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
69.30.226.220	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
37.228.91.142	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.81.157.152	France	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
94.102.49.190	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1

09-22-2016-01:10:07 to 09-22-2016-02:10:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.63.196.47	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
79.170.196.68	United Kingdom	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
158.85.253.245	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
74.208.154.12	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
92.222.142.219	France	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.46.74	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
200.59.199.229	Argentina	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
62.149.132.241	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
178.20.235.164	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.154.12	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
92.222.142.219	France	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
40.85.96.77	Ireland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.47	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
79.170.196.68	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
187.17.96.33	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
205.144.171.34	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
205.144.171.34	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
191.236.147.142	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
191.236.150.197	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
191.236.147.142	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
191.236.146.62	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
205.144.171.34	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
158.85.253.245	United States	147.237.77.176	matpash.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-22-2016-01:10:07 to 09-22-2016-02:10:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	26
79.170.196.68	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	20
50.63.196.47	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	20
74.208.154.12	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
92.222.142.219	147.237.76.86	France	navy.idf.il	SQL Injection - Select From	20
184.168.46.74	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	19
200.59.199.229	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	18
205.144.171.34	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	17
178.20.235.164	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
62.149.132.241	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	8
40.85.96.77	147.237.77.74	Ireland	law.idf.il	SQL Injection - Select From	8
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	8
87.242.112.45	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
187.17.96.33	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	7
191.236.147.142	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
191.236.150.197	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
201.216.208.137	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	4
5.135.165.89	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
93.174.93.100	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.176	United States	matpash.idf.il	ET DROP Dshield Block Listed Source	1
74.84.136.105	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
222.186.34.139	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.139	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.33	Latvia	idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
31.24.228.20	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.100	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 2048	1
221.210.200.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
123.195.227.146	147.237.72.156	Taiwan	aman.idf.il	ET SCAN Potential SSH Scan	1
211.151.3.208	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -f -sS	1
116.117.164.116	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.15.154.133	147.237.72.166	France	aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.139	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
47.88.4.204	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
191.236.146.62	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
93.174.93.100	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.100	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potenti Scan or Infection	1
221.210.200.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-01:10:07 to 09-22-2016-02:10:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
73.9.5.76	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
73.9.5.76	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	25
73.9.5.76	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	25
73.9.5.76	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
73.9.5.76	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
79.176.126.196	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
24.240.228.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
37.142.222.76	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
174.200.13.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.235	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.207.71.72	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
81.207.71.72	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
81.207.71.72	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
184.151.178.159	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.107.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
81.207.71.72	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
167.114.62.0	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
167.114.62.0	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.156	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
158.69.120.182	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.156	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.62.0	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
84.109.165.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.223.221	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.83.244	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.62.0	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
158.69.120.182	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
79.176.126.196	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.142.222.76	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
174.124.185.126	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.137.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.62.0	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.25	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
174.124.185.126	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
169.229.3.91	United States	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-22-2016-01:10:07 to 09-22-2016-02:10:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.142.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.55.36.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.222.76	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 37.142.222.76	Block	2
185.120.124.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
204.79.180.209	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
31.168.14.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
207.46.13.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
180.76.15.139	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
2.53.26.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.15.80	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
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.142.222.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
79.176.126.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.53.146.11	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
198.20.69.74	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
109.64.107.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1

09-22-2016-01:10:07 to 09-22-2016-02:10:07