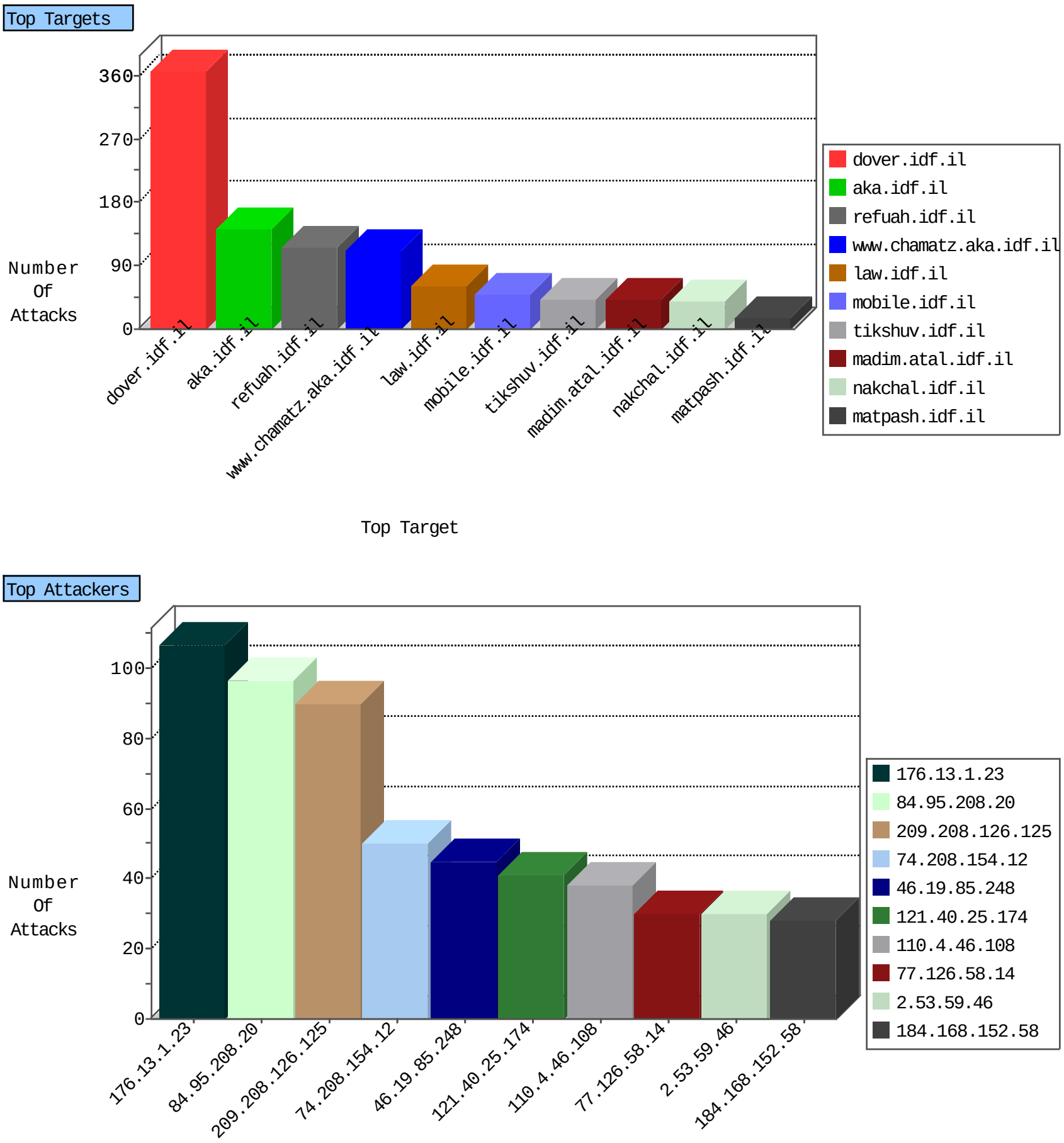
09-30-2016-12:04:07 to 09-30-2016-13:04:07

IDF Under Attack
Daily Report



09-30-2016-12:04:07 to 09-30-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.53.79	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	2
78.129.171.175	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
89.248.172.173	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
2.53.148.46	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.122.13	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
58.218.200.137	China	147.237.8.46	e.chinuch.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
110.249.208.86	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
209.126.122.13	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

09-30-2016-12:04:07 to 09-30-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.154.12	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
110.4.46.108	Malaysia	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
209.208.126.125	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
121.40.25.174	China	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.154.12	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
110.4.46.108	Malaysia	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.58	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.47	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.58	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
121.40.25.174	China	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
72.167.131.22	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.208.126.125	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
121.40.25.174	China	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.154.12	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
108.166.190.139	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

09-30-2016-12:04:07 to 09-30-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.208.126.125	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	54
74.208.154.12	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
121.40.25.174	147.237.76.42	China	refuah.idf.il	SQL Injection - Select From	20
110.4.46.108	147.237.0.34	Malaysia	tikshuv.idf.il	SQL Injection - Select From	20
50.63.196.47	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
108.166.190.139	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
184.168.152.58	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
72.167.131.22	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.152.58	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
104.207.141.110	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.73.166	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	1
62.122.99.158	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
184.105.247.204	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.207.141.110	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.64.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
62.90.215.237	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

09-30-2016-12:04:07 to 09-30-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
195.85.247.254	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
107.167.116.27	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
209.208.126.125	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	18
87.106.184.160	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
176.13.1.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
176.13.1.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
176.13.1.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
176.13.1.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
176.13.1.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
89.139.210.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	9
79.179.164.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
182.232.178.150	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.96.128.60	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.198.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.1.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.1.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.1.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
176.13.1.23	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
85.250.99.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
87.69.36.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.120.131.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.195.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.123.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.200.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.183.71.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.36.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
91.135.102.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.142.208.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.237.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
91.135.102.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-30-2016-12:04:07 to 09-30-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	43
2.53.59.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
175.44.16.72	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.16.72	Block	17
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	6
95.35.162.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
175.44.16.72	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
77.138.182.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
84.111.75.234	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
176.228.92.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.117.128.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
192.243.55.130	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
79.183.71.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.75.234	Israel	147.237.77.176	matpash.idf.il	Distributed Abnormally Long Request	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
109.67.218.20	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
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.79.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
175.44.16.72	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
37.237.201.11	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/andobx php	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
77.138.246.243	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.129	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/m/	Block	1
142.4.215.116	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
87.70.242.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
61.69.101.82	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/piwik.php	Block	1
79.177.41.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.246	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.53.143.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/null	Block	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.115.177.202	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
213.8.204.45	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
79.179.164.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9700-he/refuah.aspx	Block	1
5.29.55.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.36.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
109.67.158.238	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

09-30-2016-12:04:07 to 09-30-2016-13:04:07