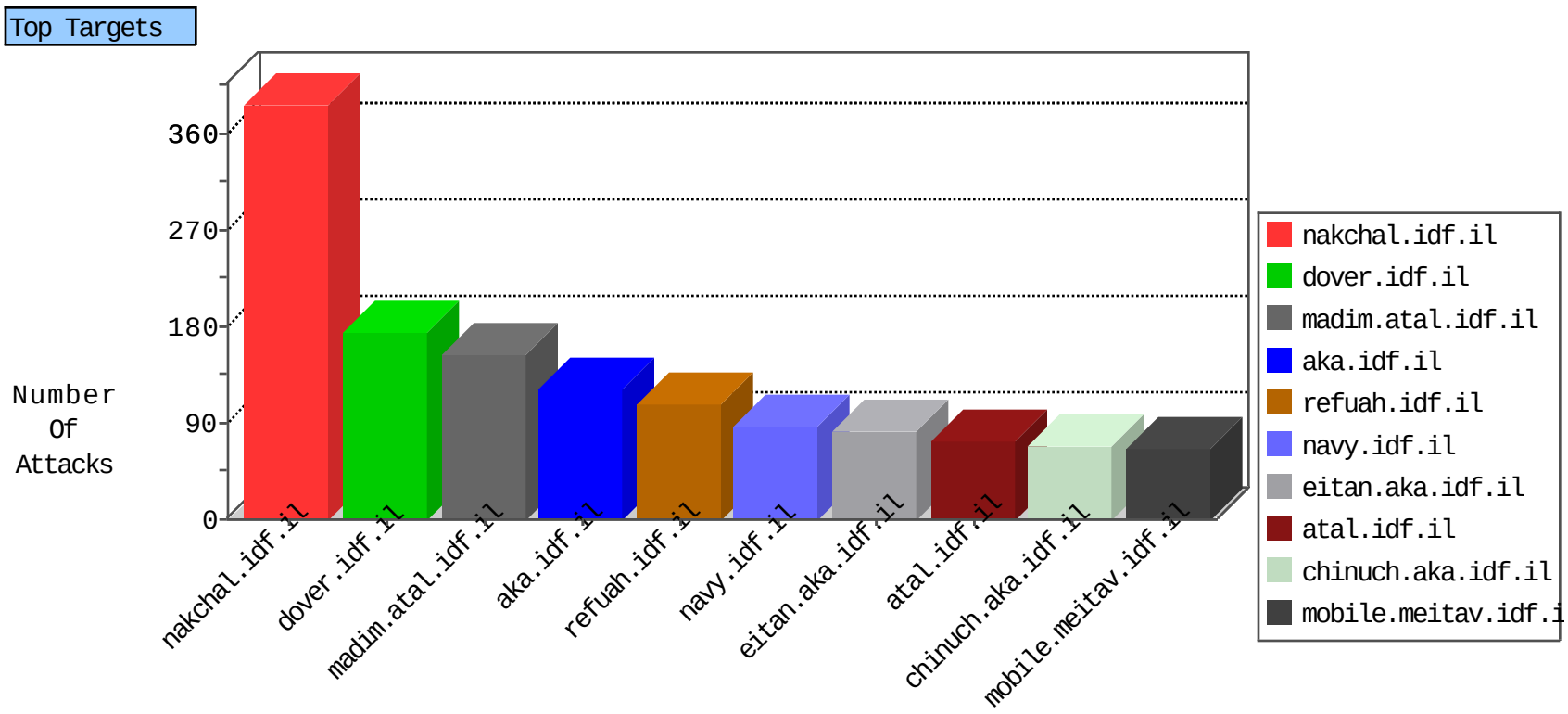
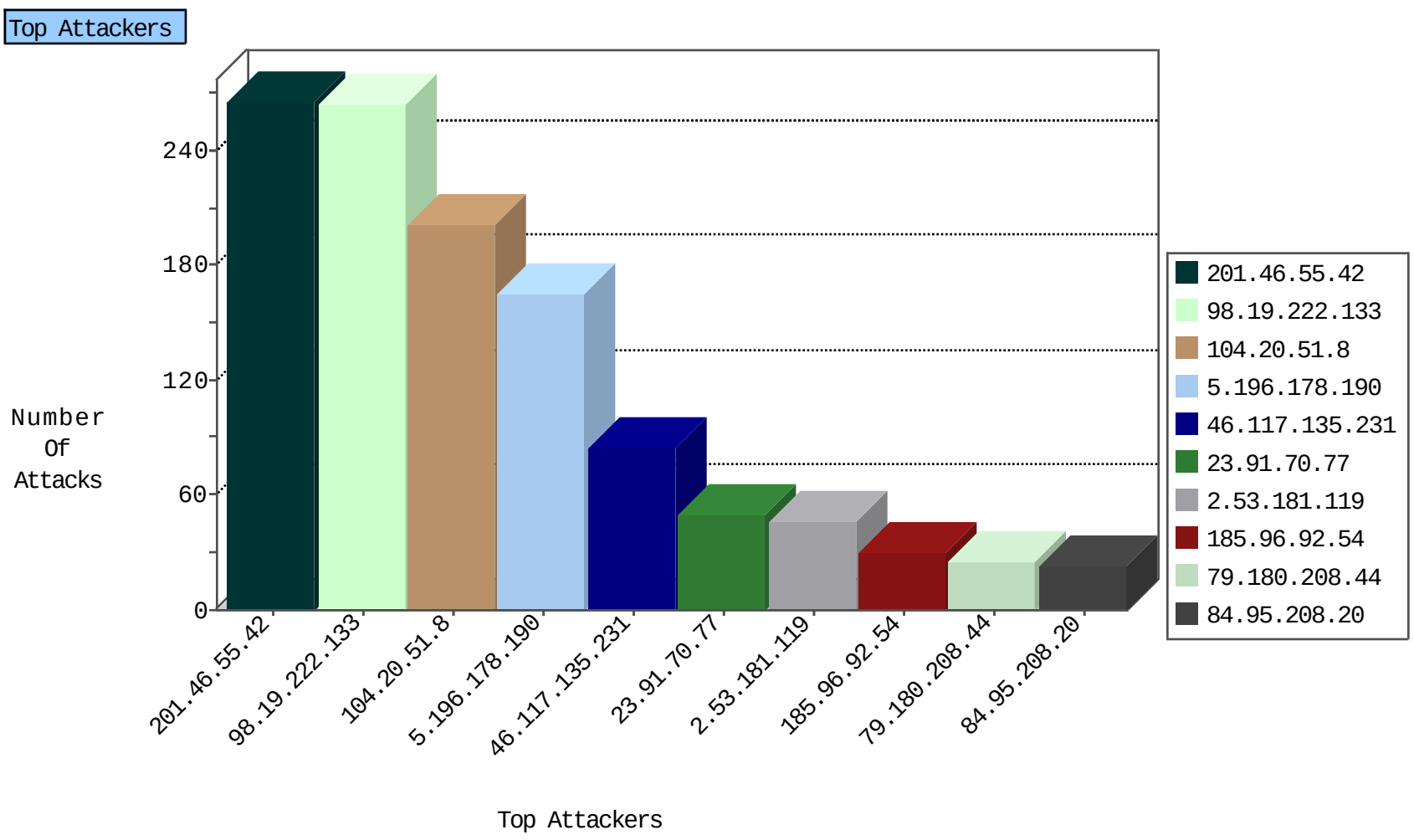
09-09-2016-10:04:05 to 09-09-2016-11:04:05

IDF Under Attack
Daily Report





09-09-2016-10:04:05 to 09-09-2016-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.136	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
2.53.170.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
2.53.138.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
71.6.158.166	United States	147.237.76.86	navy.idf.il	Black List	drop	1
173.242.116.60	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

09-09-2016-10:04:05 to 09-09-2016-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	36
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	18
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	18
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15
23.91.70.77	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
185.96.92.54	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.171.93.66	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
92.222.142.219	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
200.59.199.229	Argentina	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
191.236.150.197	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
84.20.63.93	Switzerland	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1

09-09-2016-10:04:05 to 09-09-2016-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	192
23.91.70.77	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	26
185.96.92.54	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	18
200.59.199.229	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	13
92.222.142.219	147.237.77.74	France	law.idf.il	SQL Injection - Select From	8
185.96.92.54	147.237.76.31	United Kingdom	nakchal.idf.il	SQL Injection - Select From	6
188.166.61.181	147.237.77.243	Netherlands	mobile.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
71.171.93.66	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
45.79.103.178	147.237.77.74	United States	law.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
191.236.150.197	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
87.68.33.210	147.237.76.200	Israel	eitan.aka.idf.il	GPL SCAN superscan echo	1
178.220.165.231	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
87.68.33.210	147.237.76.198	Israel	e.yohalan.idf.il	GPL SCAN superscan echo	1
163.172.129.15	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.33.210	147.237.76.196	Israel	e.sviva.idf.il	GPL SCAN superscan echo	1
87.68.33.210	147.237.76.176	Israel	test.ncore.idf.il	GPL SCAN superscan echo	1
93.158.203.149	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.33.210	147.237.76.147	Israel	chinuch.aka.idf.il	GPL SCAN superscan echo	1
93.158.203.147	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.68.33.210	147.237.76.201	Israel	e.atal.idf.il	GPL SCAN superscan echo	1
87.68.33.210	147.237.76.199	Israel	e.nakchal.idf.il	GPL SCAN superscan echo	1
178.220.165.231	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
87.68.33.210	147.237.76.197	Israel	e.himush.idf.il	GPL SCAN superscan echo	1
116.7.243.198	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.33.210	147.237.76.177	Israel	ncore.idf.il	GPL SCAN superscan echo	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
87.68.33.210	147.237.76.148	Israel	gqcenter.aka.idf.i	GPL SCAN superscan echo	1
93.158.203.149	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.33.210	147.237.76.86	Israel	navy.idf.il	GPL SCAN superscan echo	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
87.68.33.210	147.237.76.202	Israel	e.halag.idf.il	GPL SCAN superscan echo	1

09-09-2016-10:04:05 to 09-09-2016-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	31
79.180.208.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.85.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
5.196.178.190	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.196.178.190	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.196.178.190	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.196.178.190	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.196.178.190	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.196.178.190	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
5.196.178.190	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
5.196.178.190	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
81.154.219.52	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.83.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
95.35.224.126	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
104.20.51.8	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.20.51.8	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.20.51.8	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.20.51.8	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.20.51.8	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.20.51.8	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
176.13.9.29	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
31.168.232.218	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
104.20.51.8	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.20.51.8	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
192.115.22.115	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.20.51.8	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
95.35.224.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.13.114.68	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-09-2016-10:04:05 to 09-09-2016-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.135.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.181.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
77.139.212.165	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.121.109.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.46.41.179	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
77.138.190.29	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
31.210.187.105	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
45.79.103.178	United States	147.237.77.74	law.idf.il	Malformed URL	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.177.175.162	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.130	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
188.166.61.181	Netherlands	147.237.77.243	mobile.idf.il	Unauthorized HTTP Method	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	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
37.26.149.144	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
77.138.221.14	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.221.14	Block	1
185.89.217.226	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
45.79.103.178	United States	147.237.77.74	law.idf.il	Multiple Malformed HTTP Header Line from 45.79.103.178	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
79.180.208.44	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
188.166.61.181	Netherlands	147.237.77.243	mobile.idf.il	Unauthorized Method OPTIONS for /	Block	1
77.125.11.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
84.108.11.88	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.19.86.29	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.149.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
77.138.221.14	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/robots.txt	Block	1
185.89.217.229	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/	Block	1
45.79.103.178	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 45.79.103.178	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
2.53.150.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.22.115	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.190.29	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
87.68.41.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/70009.doc	Block	1
185.89.217.230	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
45.79.103.178	United States	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 45.79.103.178	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
89.237.79.64	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
46.116.104.105	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1

09-09-2016-10:04:05 to 09-09-2016-11:04:05