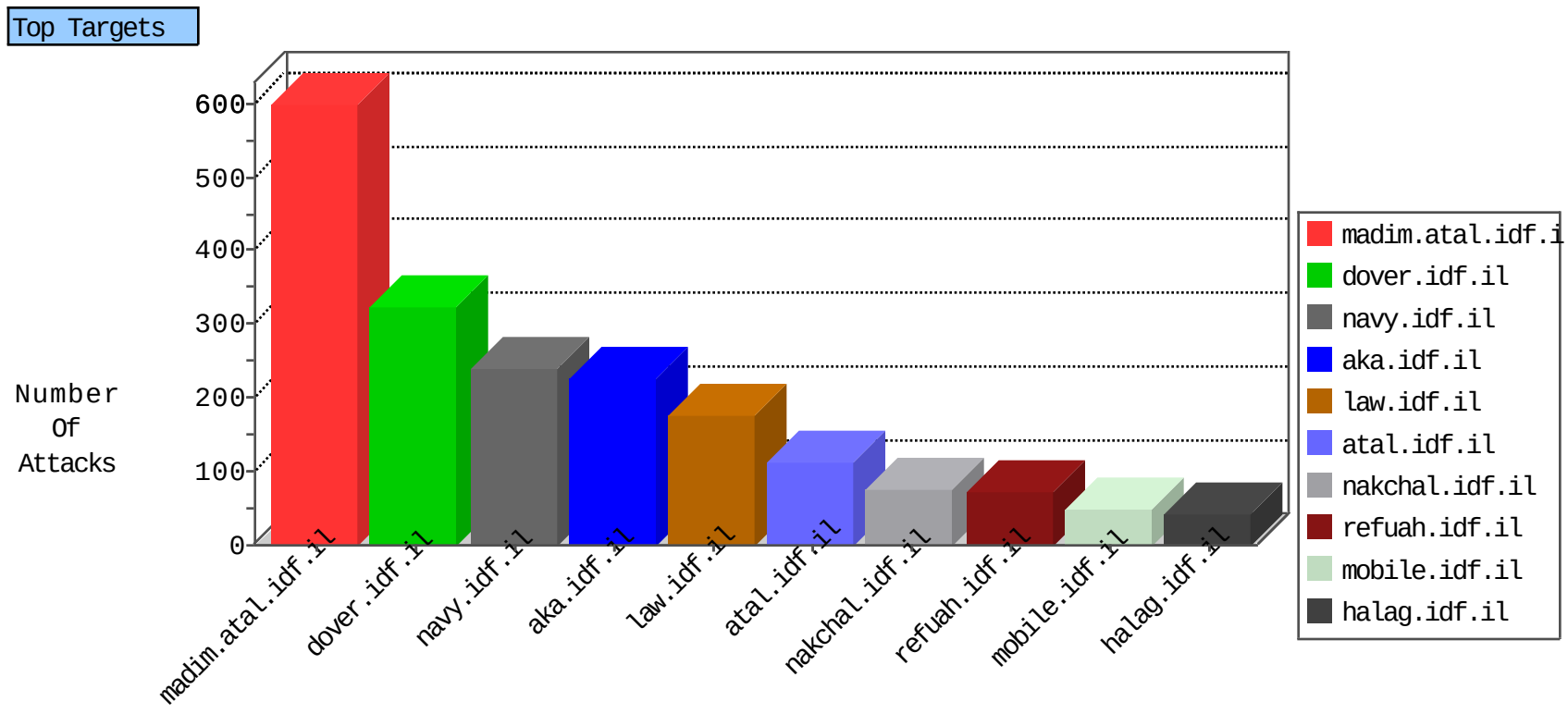
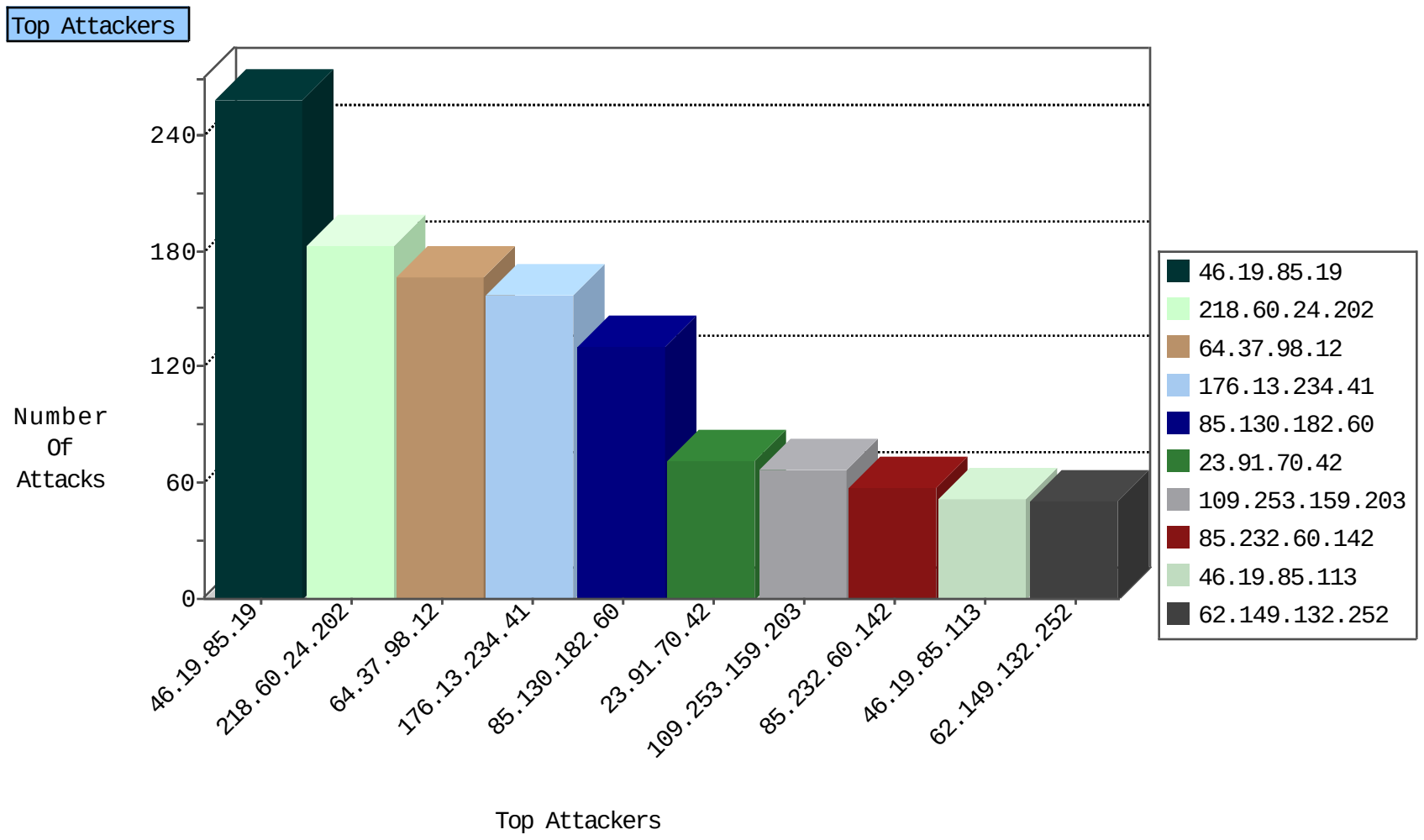
09-07-2016-11:04:06 to 09-07-2016-12:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-07-2016-11:04:06 to 09-07-2016-12:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.130.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
192.116.255.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
198.27.100.198	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Black List	drop	1

09-07-2016-11:04:06 to 09-07-2016-12:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.228.38.74	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
85.232.60.142	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
23.91.70.42	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
62.149.132.252	Italy	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
195.8.208.118	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.232.60.142	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.42	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.69.119.162	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.115.226.16	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
62.149.132.252	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
67.228.38.74	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
95.211.70.193	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
110.4.46.108	Malaysia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
61.220.26.201	Taiwan	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
74.208.230.195	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
95.211.70.193	Netherlands	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
75.56.235.20	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
103.238.138.4	Indonesia	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-07-2016-11:04:06 to 09-07-2016-12:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.91.70.42	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	53
85.232.60.142	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	40
62.149.132.252	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	33
67.228.38.74	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	33
195.8.208.118	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	21
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	15
209.15.196.171	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	11
213.115.226.16	147.237.76.42	Sweden	refuah.idf.il	SQL Injection - Select From	9
158.69.119.162	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	4
82.81.137.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
103.207.36.84	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
80.246.136.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.110.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.184.122	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
191.96.112.40	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.166.61.181	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
45.56.108.106	147.237.77.179	United States	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
23.91.75.231	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.43.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
88.202.218.230	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.235.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.210.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.38.68.132	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.112.40	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.42	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
150.242.238.99	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-07-2016-11:04:06 to 09-07-2016-12:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.143.77.23	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
85.130.182.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
213.57.244.226	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
85.130.182.60	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
85.130.182.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
85.130.182.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
85.130.182.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
64.37.98.12	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
64.37.98.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
64.37.98.12	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
64.37.98.12	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.12	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.85.56	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.37.98.12	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
85.130.182.60	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
185.87.183.56	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
64.37.98.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
64.37.98.12	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.87.183.56	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
80.178.220.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
218.60.24.202	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
176.13.243.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.59.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
218.60.24.202	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.117.136.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.230.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
218.60.24.202	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.179.219.218	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
209.197.16.156	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
218.60.24.202	China	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.240.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.202	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.202	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.202	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
198.27.100.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.87.183.56	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.202	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.202	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
218.60.24.202	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.37.98.12	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
64.37.98.12	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
218.60.24.202	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
64.37.98.12	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-07-2016-11:04:06 to 09-07-2016-12:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	257
176.13.234.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	158
109.253.159.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
109.253.245.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
87.68.242.80	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 87.68.242.80	Block	15
185.32.179.48	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.32.179.48	Block	11
37.26.147.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.147.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.234.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	5
176.13.243.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
77.138.156.38	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	4
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.229.53.32	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/647-2336-he/patzar.aspx	Block	3
213.57.147.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/giyus	Block	2
89.139.128.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
185.32.179.48	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
87.71.23.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txt in www.aka.idf.il/main/sachar/	None	1
2.55.53.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
188.166.61.181	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
79.177.146.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
37.26.149.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.110.55.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	1
185.32.179.48	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1513	Block	1
157.55.39.20	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
87.71.23.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
10.112.50.12		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim/	Block	1
213.57.244.226	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Malformed HTTP Header Line 3	Block	1
84.229.53.32	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/580-he/patzar.aspx	Block	1
212.179.223.235	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.125.0.144	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
188.166.61.181	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 188.166.61.181 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
213.57.244.226	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
82.80.33.138	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1

09-07-2016-11:04:06 to 09-07-2016-12:04:06