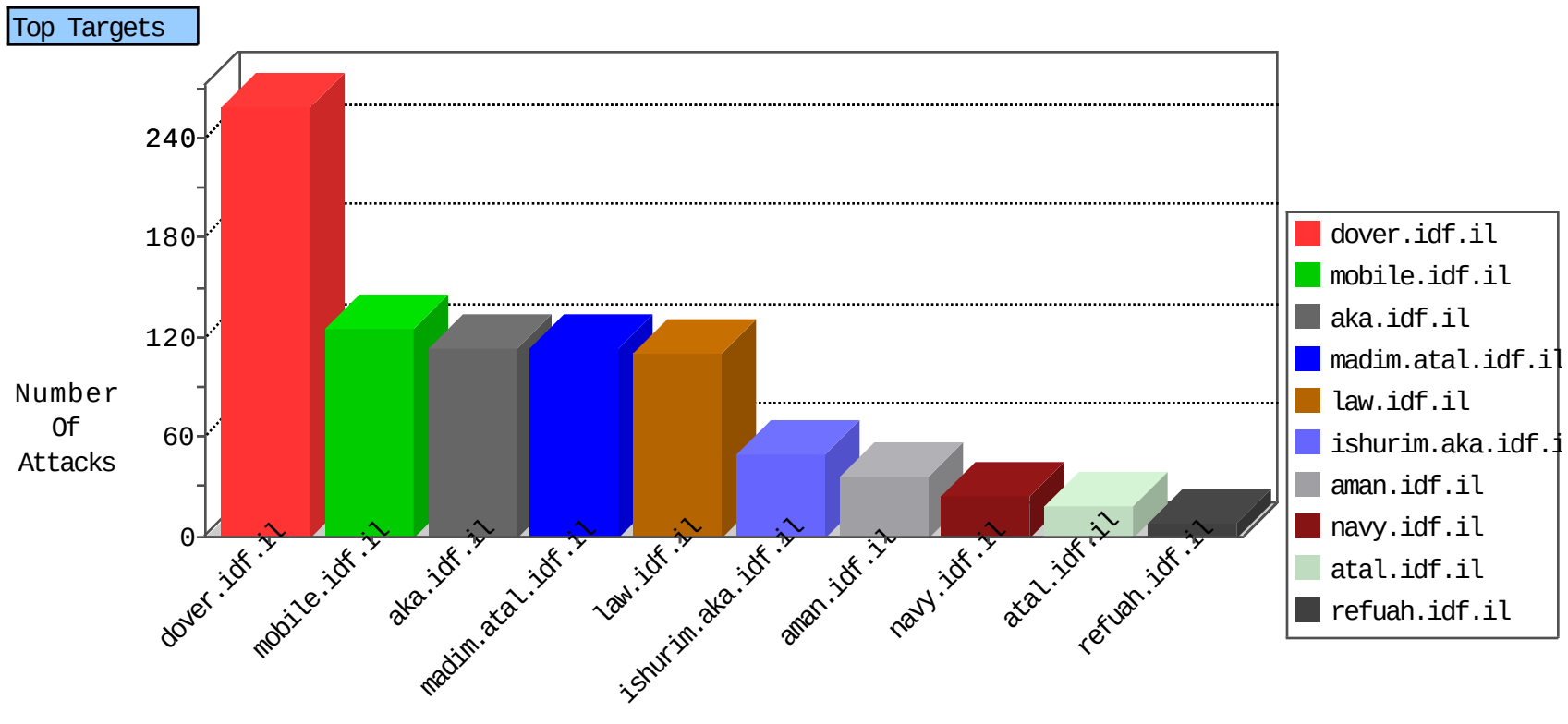
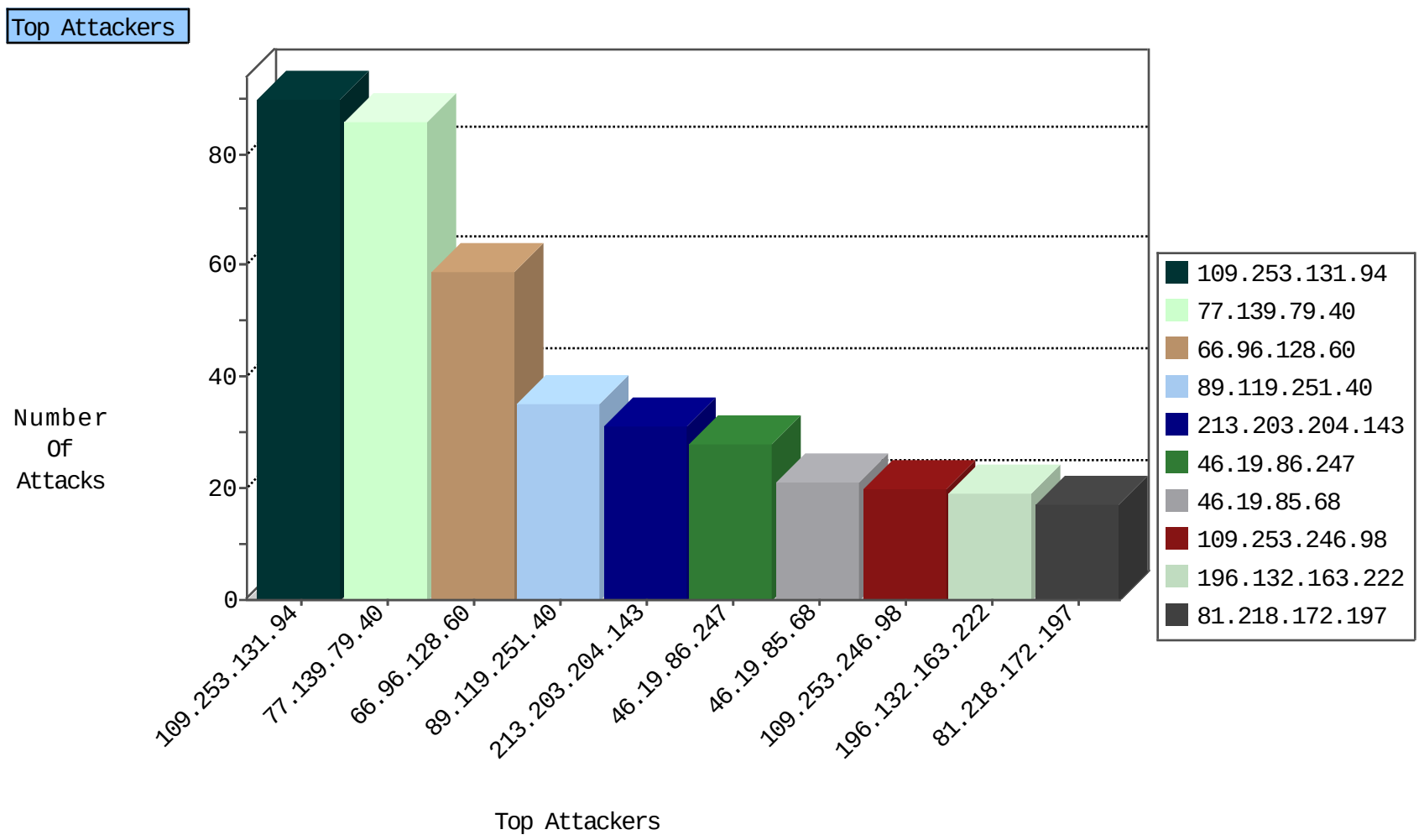
09-01-2016-13:04:07 to 09-01-2016-14:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-01-2016-13:04:07 to 09-01-2016-14:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.136.59	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
141.226.161.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.168.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
212.25.74.130	Israel	147.237.77.233	atal.idf.il	Black List	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
5.189.186.243	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
212.179.64.162	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.177	ncore.idf.il	Black List	drop	1
185.93.185.10	Ukraine	147.237.76.200	eitan.aka.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	1
5.189.186.243	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
37.26.146.206	Israel	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
5.189.186.243	Germany	147.237.76.30	himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-01-2016-13:04:07 to 09-01-2016-14:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.203.204.143	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.203.204.143	Germany	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
66.96.128.60	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
40.85.96.77	Ireland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.9.88.103	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
213.203.204.143	Germany	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
27.251.116.34	India	147.237.77.74	law.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
83.168.250.50	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
40.85.96.77	Ireland	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-01-2016-13:04:07 to 09-01-2016-14:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.131.94	147.237.77.243	Israel	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	40
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	35
213.203.204.143	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	19
84.93.100.67	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
79.181.23.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.86.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.170.171.141	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.32.14.110	147.237.77.226	Colombia	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.63.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.32.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.101.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.31.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.92.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.3.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.1.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.65.240.98	147.237.8.50	Indonesia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.106.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.47.12.162	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
8.37.237.159	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.120.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
101.250.183.95	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-01-2016-13:04:07 to 09-01-2016-14:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.131.94	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	50
89.119.251.40	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
196.132.163.222	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.53.10.37	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
31.154.101.212	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
93.172.60.79	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.229.10.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.253.246.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
84.229.10.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.253.246.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.110.178.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
50.63.197.145	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
75.56.235.20	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
81.218.172.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.172.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.218.172.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.165.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.8.61.110	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
138.246.253.19	Germany	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.253.246.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
31.168.165.230	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
46.19.86.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.110.178.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
82.102.168.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
138.246.253.19	Germany	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
89.138.227.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
138.246.253.19	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
195.60.235.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.149.153	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.164.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.117.85.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.177.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.124.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.178.159	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-01-2016-13:04:07 to 09-01-2016-14:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.79.40	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
132.74.145.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
176.13.245.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.195.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.233.14	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/images/shared/err_page.png	Block	3
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.20.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.37.64	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
176.13.233.14	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/320-he/patzar.aspx	Block	2
109.253.141.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.133.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.43.198	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.183.32.48	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
82.135.222.210	Lithuania	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
77.138.106.94	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	1
132.71.96.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl81 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.76.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21998-he/idfgdover.aspx	Block	1
98.139.14.250	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 98.139.14.250	Block	1
37.26.147.241	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
80.230.216.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
71.119.208.103	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.117.85.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/haredim/contactus.aspx	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
2.53.45.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
98.139.14.250	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/sip_storage/	Block	1
80.246.130.12	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
71.119.208.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
65.55.210.241	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.66.183	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.64	Block	1
78.192.78.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
146.198.184.233	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kiosk	Block	1
109.64.122.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
80.246.130.78	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.127.8.65	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.64.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/home/default.aspx	Block	1
84.108.176.83	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

09-01-2016-13:04:07 to 09-01-2016-14:04:07