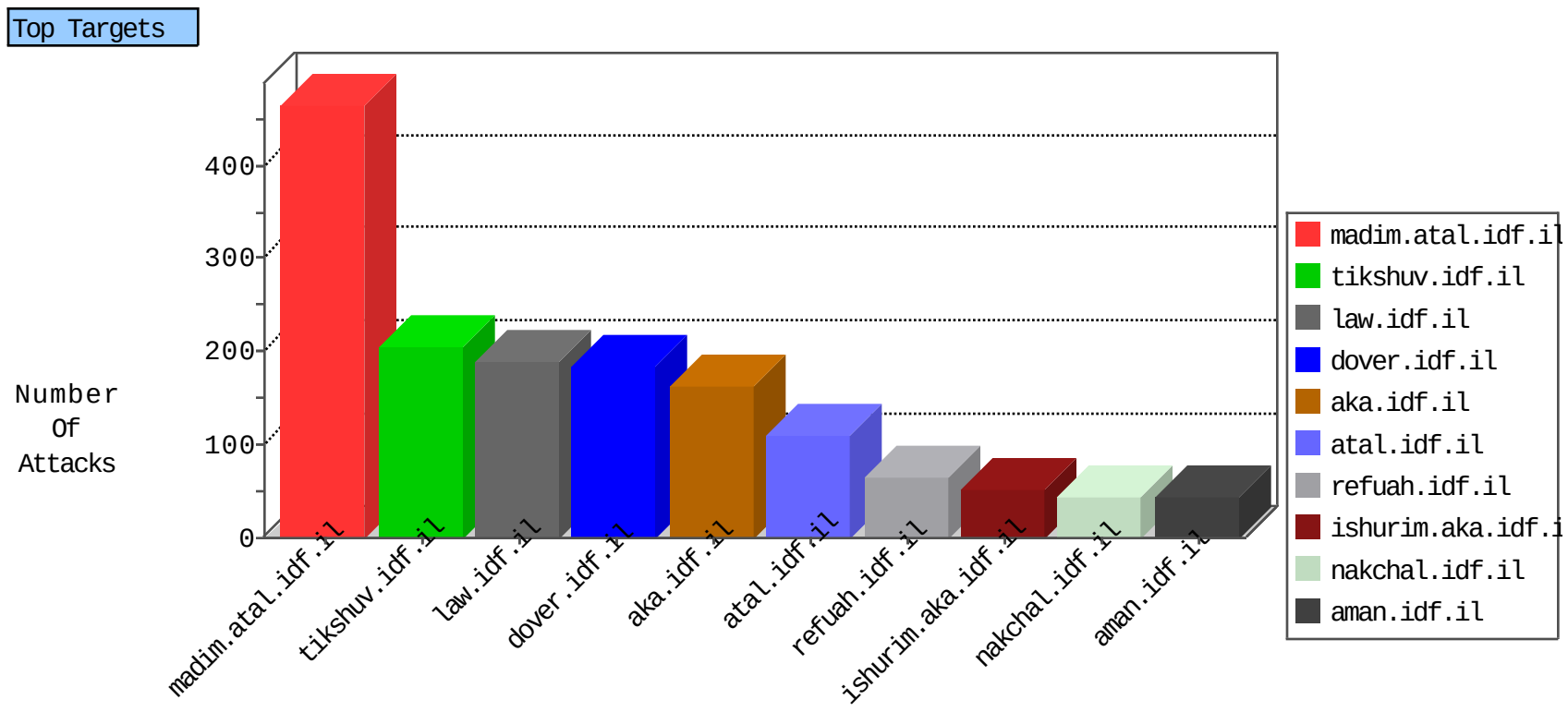
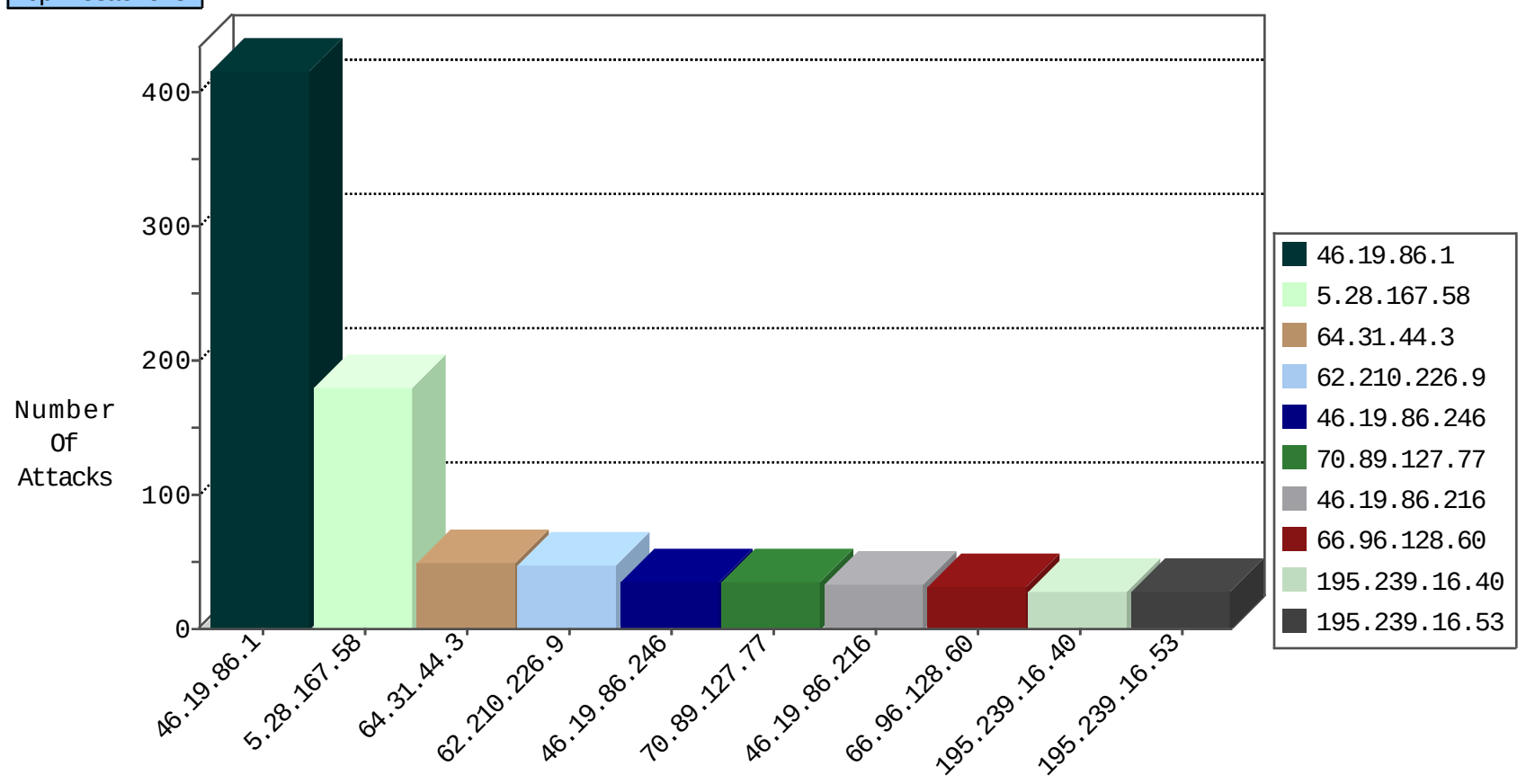
02-15-2016-23:04:05 to 02-16-2016-00:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-15-2016-23:04:05 to 02-16-2016-00:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
219.148.198.41	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
104.148.100.2	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
183.164.106.62	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-15-2016-23:04:05 to 02-16-2016-00:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.31.44.3	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
62.210.226.9	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.106.114.136	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
64.31.44.3	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
24.47.146.194	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
70.89.127.77	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
62.210.226.9	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.140.210.83	Germany	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
178.63.18.196	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.77	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
24.47.146.194	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.173.233.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.185.43.135	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.89.127.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
70.89.127.78	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
94.22.47.242	Finland	147.237.77.176	matpash.idf.il	C106: HTTP: majestic bot	Block	1
70.89.127.78	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.90	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-15-2016-23:04:05 to 02-16-2016-00:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.226.9	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	36
64.31.44.3	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	26
70.89.127.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	26
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
24.47.146.194	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	14
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	12
184.106.114.136	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
70.89.127.78	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.140.210.83	147.237.76.42	Germany	refuah.idf.il	SQL Injection - Select From	6
216.185.43.135	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	6
184.173.233.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
178.63.18.196	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.177.121.227	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
166.63.124.156	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
54.183.197.26	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
40.118.160.70	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.182.242.200	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
54.183.197.26	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
40.118.160.70	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

02-15-2016-23:04:05 to 02-16-2016-00:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
79.180.209.228	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
149.78.21.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.128	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.102.9.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
177.185.192.98	Brazil	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
66.96.128.60	United States	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	12
109.253.213.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.10.177	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.115.177.203	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
190.104.131.126	Paraguay	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.5.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.10.125.228	Hungary	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
216.185.43.135	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
85.64.234.152	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
46.19.86.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.56.38	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.167.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.128	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.227.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.227.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.187.53	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.58	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
177.185.194.92	Brazil	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
196.217.19.211	Morocco	147.237.77.176	matpash.idf.il	drop		drop	4
85.64.234.152	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.67	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.119.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.54.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.133.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.76.127.111	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.228.216.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-15-2016-23:04:05 to 02-16-2016-00:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.1	Block	273
5.28.167.58	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.167.58	Block	178
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.1	Block	19
185.32.179.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.13.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
84.228.13.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	4
46.120.250.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.250.174	Block	3
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.56.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.186.16.244	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
31.168.240.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.10.178	Portugal	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
83.130.100.33	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
46.120.250.174	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
5.29.163.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ufi/reaction/	Block	1
192.157.245.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
79.179.34.244	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
104.128.144.131	Canada	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
5.29.163.189	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
216.185.43.135	United States	147.237.72.166	aka.idf.il	Multiple signatures from 216.185.43.135	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/	Block	1
133.130.58.190	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/888.pdf	Block	1
93.186.16.245	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.209.228	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
199.30.24.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.250.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
185.25.148.240	Poland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
104.128.144.131	Canada	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
46.19.86.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.195.191	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
5.29.163.189	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ajax/updatestatus.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx	Block	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.32	Block	1
95.86.117.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
5.28.167.58	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
216.185.43.135	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
46.254.166.16	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	1
185.25.148.240	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on testp3.pospr.waw.pl/testproxy.php	Block	1
109.111.112.73	Andorra	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.111.112.73 (Open Mode)	None	1
5.29.163.189	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.163.189	Block	1
93.173.49.247	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.49.14.190	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
46.117.117.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/dover/site/mainpage.asp	Block	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.19.85.240	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1

02-15-2016-23:04:05 to 02-16-2016-00:04:05