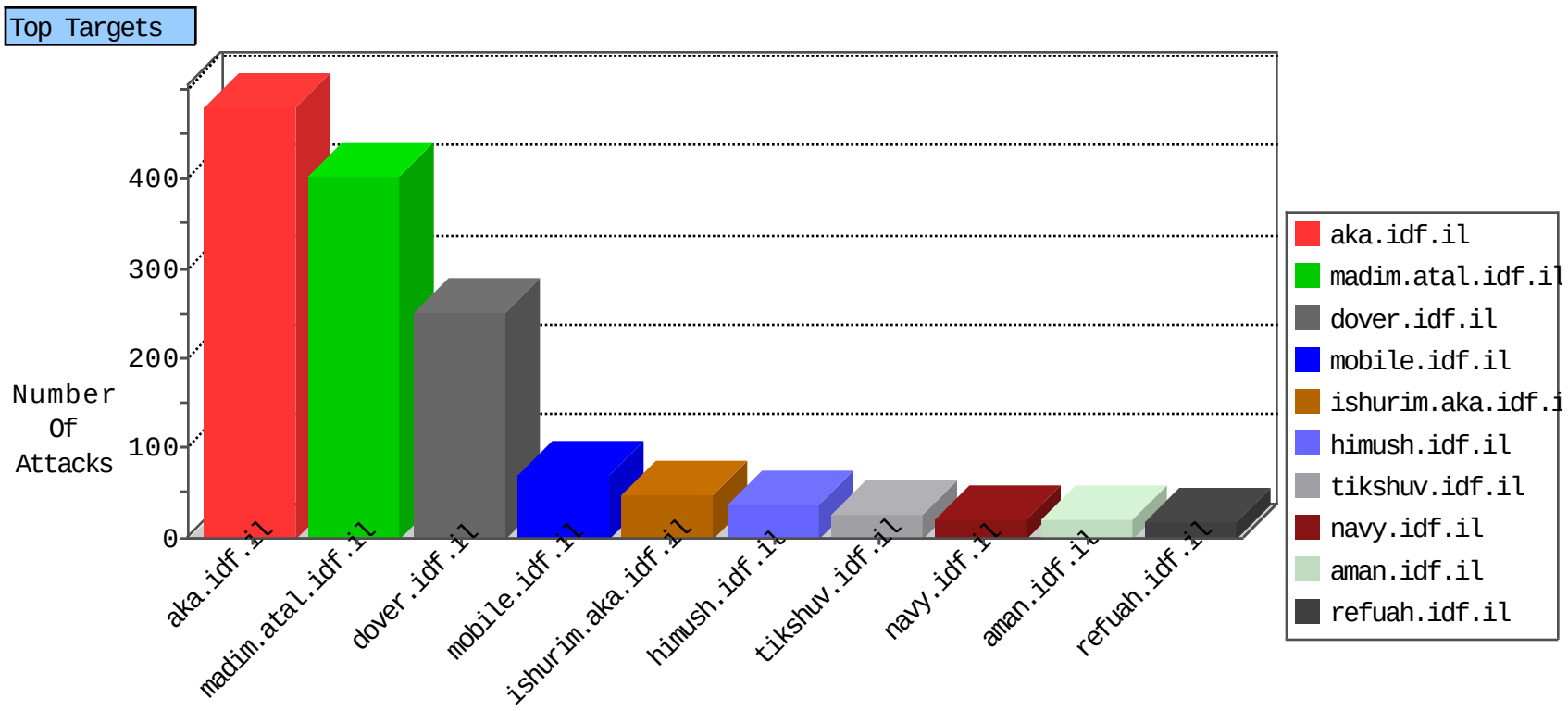
03-02-2016-11:04:07 to 03-02-2016-12:04:07

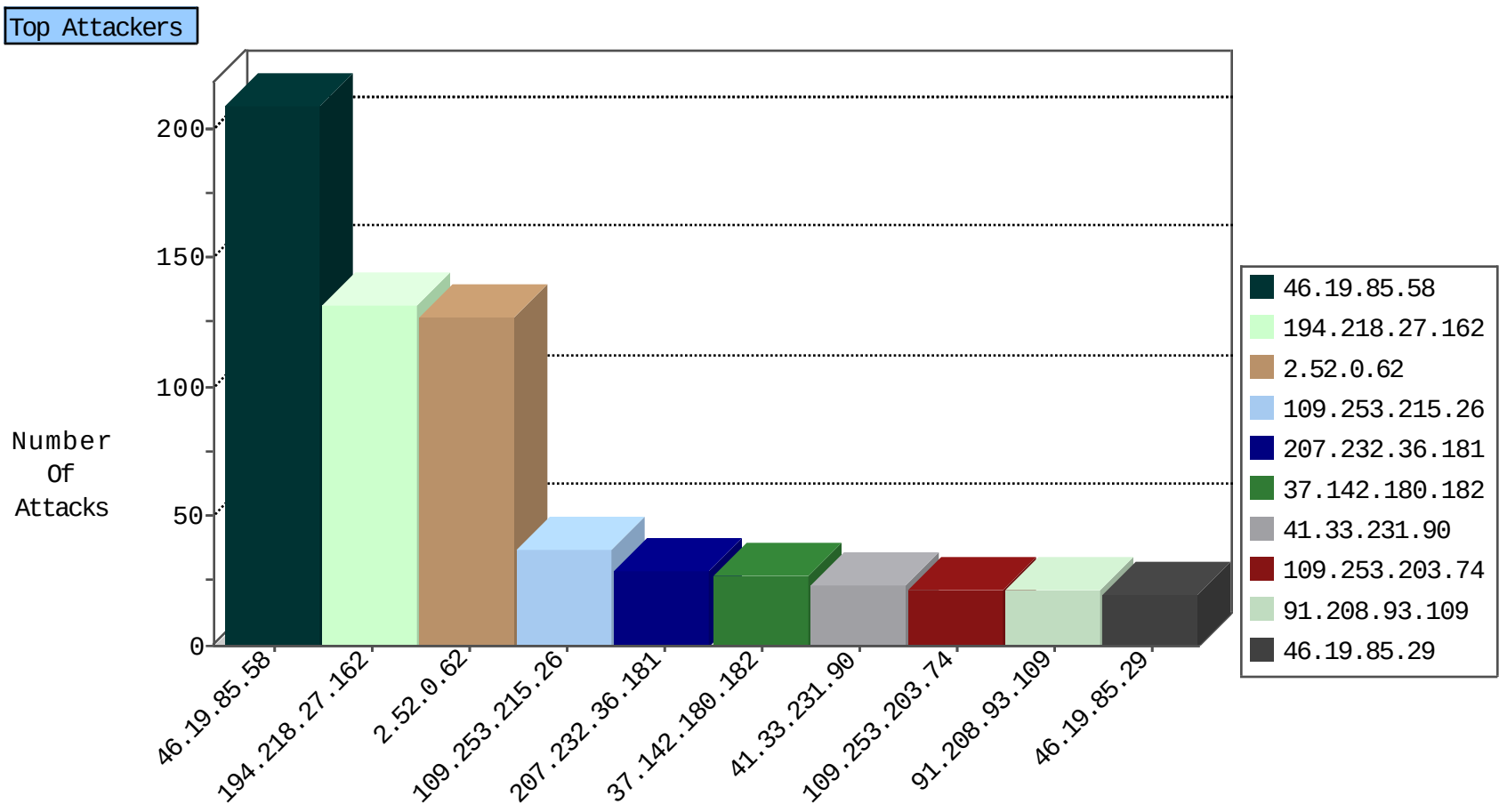
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-02-2016-11:04:07 to 03-02-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	275
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
93.157.87.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
95.86.67.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.65.7.227	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.145.208.244	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
80.246.136.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
179.153.197.122	Brazil	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
192.99.63.194	Canada	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
24.133.75.0	Turkey	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

03-02-2016-11:04:07 to 03-02-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
178.203.146.227	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
192.118.73.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.246.133.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.65	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.52.3.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.246.133.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
5.9.85.4	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

03-02-2016-11:04:07 to 03-02-2016-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
189.254.90.133	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
134.191.232.71	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
94.230.93.236	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.146.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.99.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.210.233.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.238	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.73.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.172.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.254.90.133	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.33.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.120.47	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
85.130.216.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.173.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
199.101.186.238	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.154.94.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.254.90.133	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.45.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-02-2016-11:04:07 to 03-02-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	88
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
91.208.93.109	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
109.253.131.81	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.142.180.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
109.67.25.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
193.16.147.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.33.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.139.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.26.146.244	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.64.16.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.116.105.90	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
2.52.162.128	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.177.196.87	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
37.142.180.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
95.86.67.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.0.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.96		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.32.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.226.48.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.33.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.157.87.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.157.87.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
141.0.14.78	Europe	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.120.174.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.3.146	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	5
46.19.86.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
80.246.139.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.142.180.182	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.48.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.2.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.126.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.186.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.43.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.139.23.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.141	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.169.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.50.232	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	209
2.52.0.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
109.253.215.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
5.29.199.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.199.233	Block	17
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	9
2.54.17.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
80.246.139.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	4
2.52.143.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.254.244	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.90.254.244	Block	3
194.90.254.244	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
185.32.179.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.210.233.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.32.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.94.76.213	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
5.29.163.189	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.29.163.189	Block	2
2.54.32.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.245	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
157.55.39.58	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.58	Block	2
2.54.3.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.8.198	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
95.86.116.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.148	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	NULL Character in URL r»°[[Ʊ#7ך˜:*]]vŒ8Ùe•[[#30]]¾r[[ƥ¸ƛÐ#0˙]]œ2‘—	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
134.191.232.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
107.150.42.34	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
87.68.66.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
31.13.113.78	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	1
66.249.81.215	Russian Federation	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.39	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
212.143.122.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.201.163	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning V1	Block	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
185.6.64.114	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
37.26.148.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	1
157.55.39.21	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/21012011masaiyot.aspx	Block	1
5.29.163.189	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.54.1.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
107.150.42.36	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to www.yun.ph/	Block	1