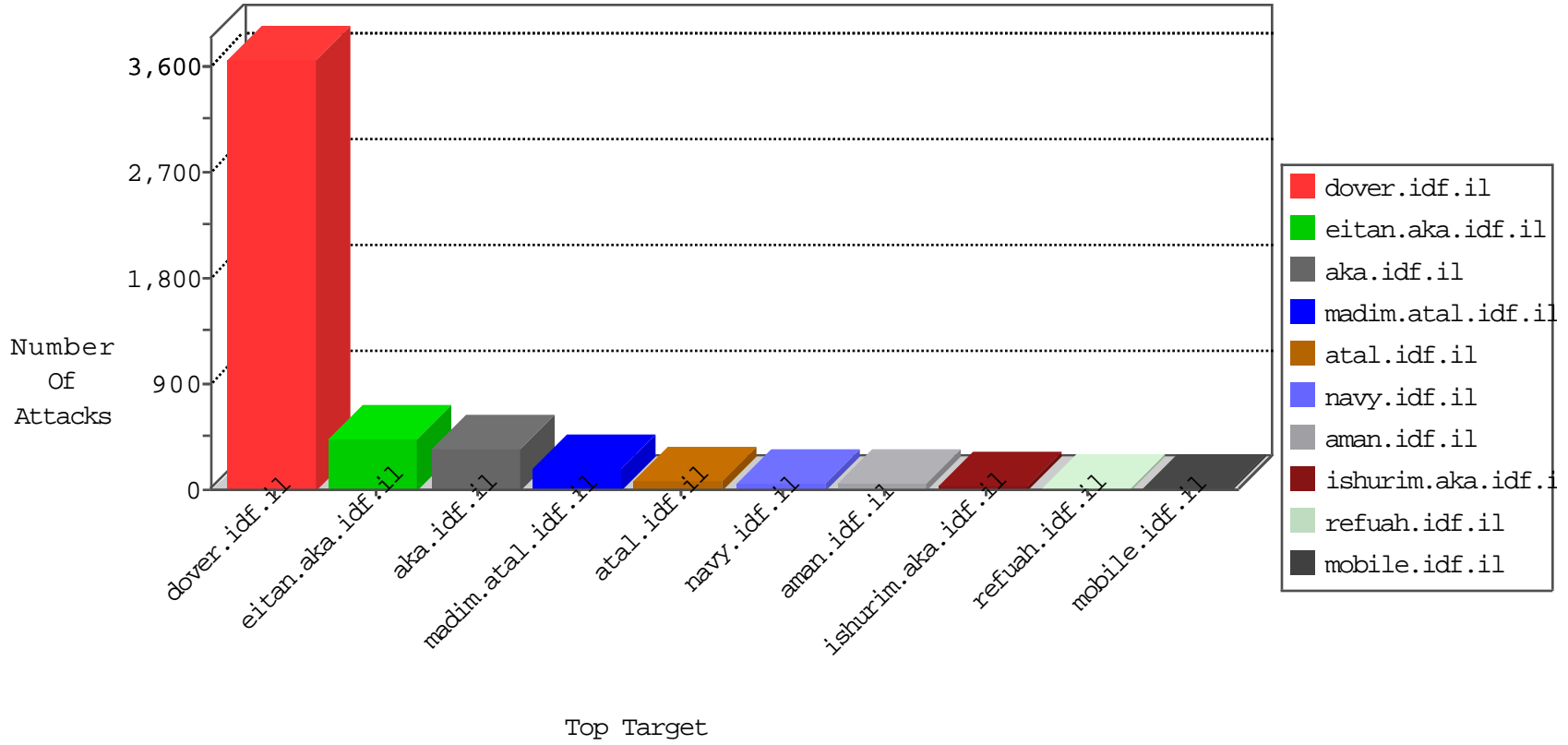


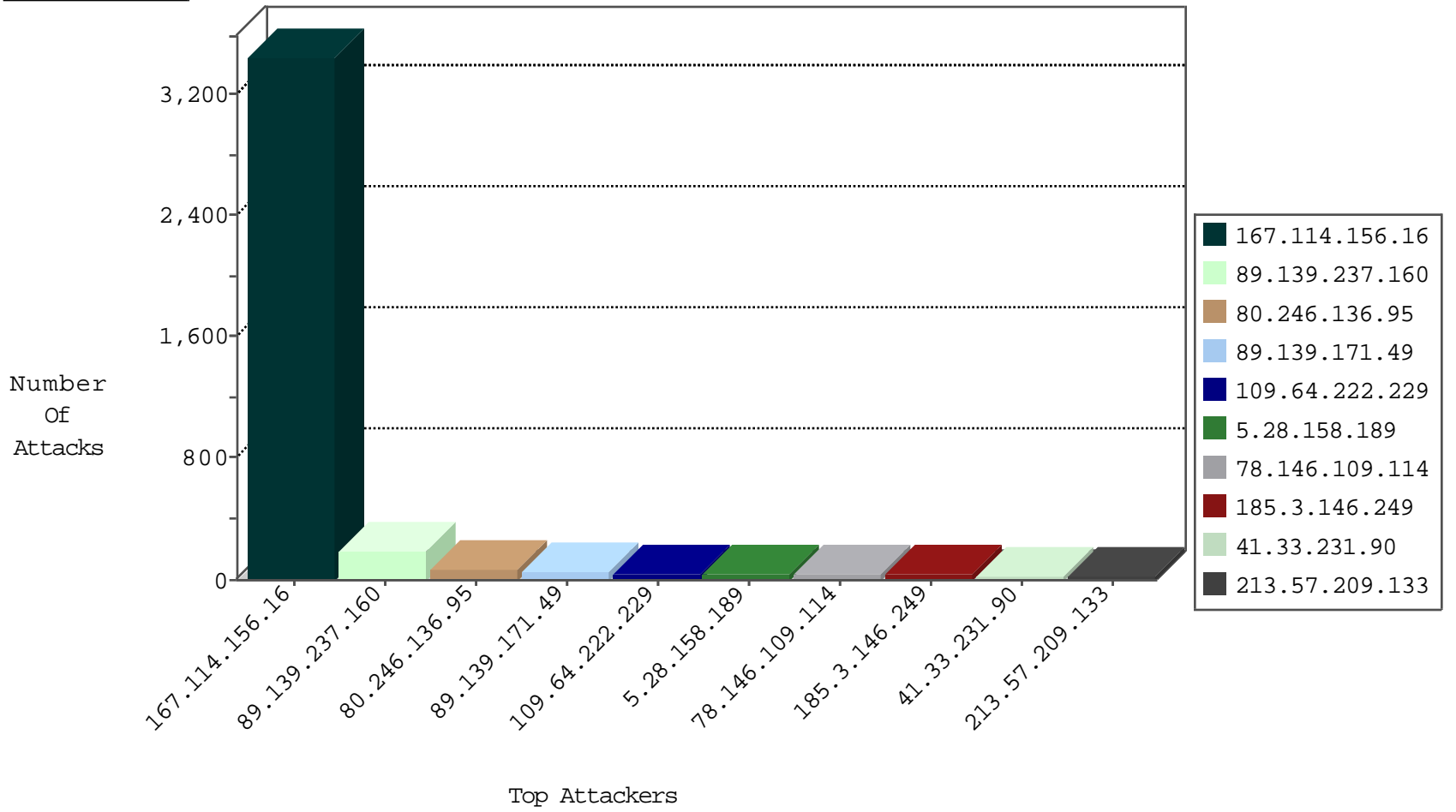
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3438
82.81.6.86	Israel	147.237.77.216	dover.idf.il	Invalid I4 Header Length	drop	7
82.81.6.86	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-trafl	forward	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
95.25.14.10	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
202.112.51.96	China	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	forward	2
95.25.14.10	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
202.112.51.96	China	147.237.72.156	aman.idf.il	block-sp-trafl	forward	2
62.138.3.55	Germany	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
78.188.169.77	Turkey	147.237.76.176	test.ncore.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
78.188.169.77	Turkey	147.237.76.177	ncore.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
78.188.169.77	Turkey	147.237.77.179	e.mazi.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1
82.81.6.86	Israel	147.237.77.233	atal.idf.il	Invalid I4 Header Length	drop	1
78.188.169.77	Turkey	147.237.76.38	e.e.meitav.idf.il	ID-OpenSSL-Heartbeat-ex1	dest-reset	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.145.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.88.198.104	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
172.240.88.34	United States	147.237.76.86	navy.idf.il	C1000003: HTTP: phpMyAdmin access	Block	2
77.126.12.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.107	France	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
111.202.102.74	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.107	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
194.146.225.239	147.237.0.16	France	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.237.160	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
89.139.171.49	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
78.146.109.114	United Kingdom	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
185.3.146.249	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.109.101.91	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	27
66.249.81.175	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	25
82.80.178.39	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.103.149	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
66.249.81.179	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
176.63.127.145	Hungary	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
149.78.43.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
31.154.151.223	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.181.135.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.81.183	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
95.25.14.10	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
109.64.50.224	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.156.93	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.10.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.132.229.226	United Kingdom	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
73.182.232.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.28.158.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
216.72.34.205	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.254.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.67.173.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
166.173.250.150	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.253.138.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.211.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.150.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.166.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.227.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.201.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
31.154.242.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.92.23.58	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.159.53	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.158.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
79.177.105.50	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
188.120.148.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
88.128.80.52	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.53.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.144.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.53.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.28.158.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
65.55.210.22	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.191	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

04-17-2016-20:04:08 to 04-17-2016-21:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.17.55	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.116.62.204	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.64.222.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
213.57.209.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
5.28.158.189	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.158.189	Block	11
176.228.218.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/iturim/asp/	Block	7
176.228.218.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/teuda.asp	Block	7
213.8.204.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.69.41	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 95.86.69.41	Block	5
109.253.208.46	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.253.208.46	Block	4
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.130.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.33.104	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.180.33.104	Block	3
2.53.129.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.226.234	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on kosher-kravi.idf.il/1193-he/orchotaspx	Block	2
213.57.104.147	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.218.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.26.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
89.139.237.160	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
78.188.169.77	Turkey	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
172.240.88.34	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
95.86.112.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
5.28.140.23	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
79.181.135.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
193.169.52.111	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
149.78.239.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/926-he/refuah.aspx	Block	1
109.253.208.46	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
202.112.51.96	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to bter.com/	Block	1
85.250.90.93	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
78.188.169.77	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
172.240.88.34	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/php/index.php	Block	1
46.19.86.255	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/71725.pdf	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
194.146.225.239	France	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.182.215.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
157.55.2.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
207.46.13.53	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
87.70.48.204	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
78.188.169.77	Turkey	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
109.186.54.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/	Block	1
5.28.158.189	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/login.aspx	Block	1
217.69.133.6	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
194.146.225.239	France	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
157.55.39.243	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1065-en/dover.aspx	Block	1
46.19.85.128	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1