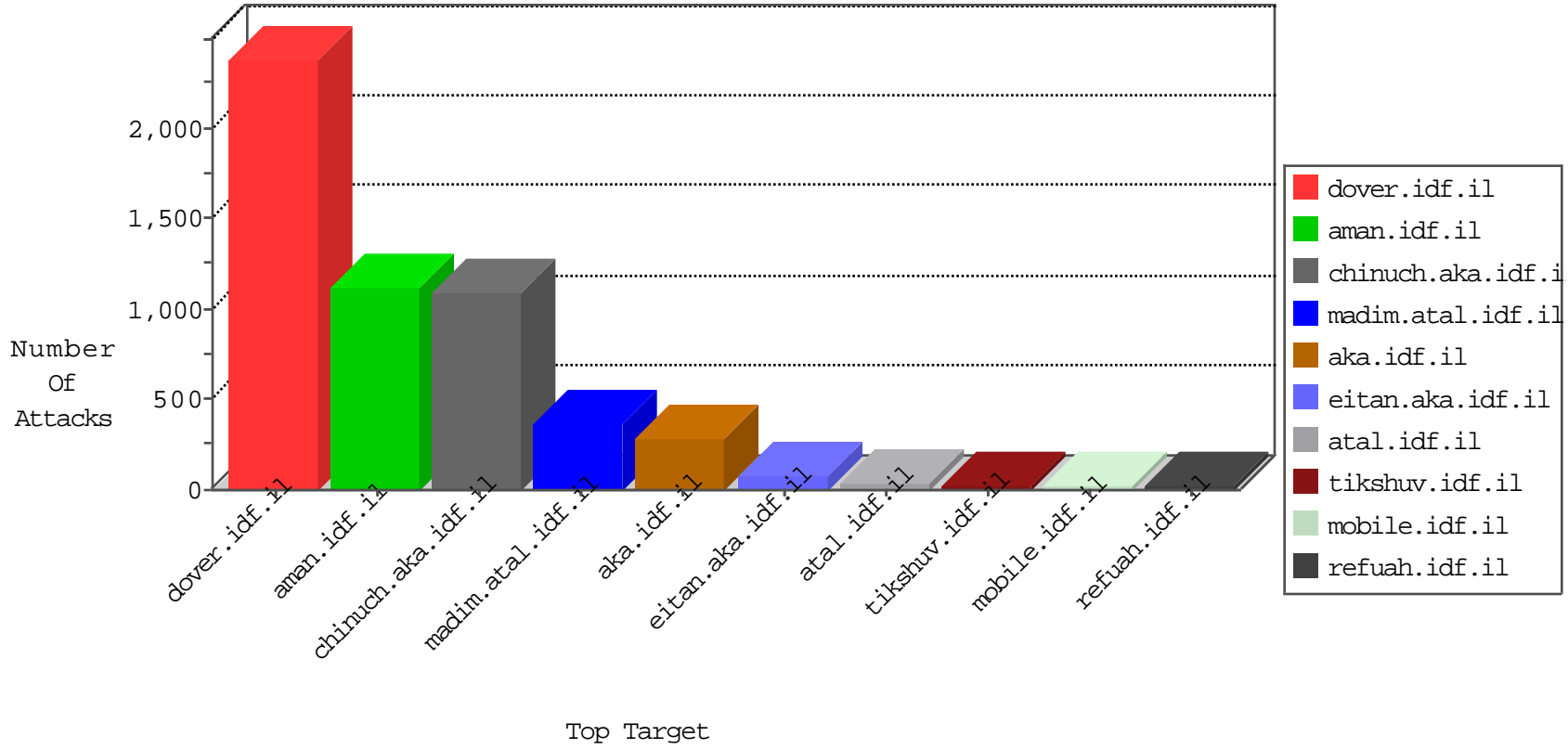


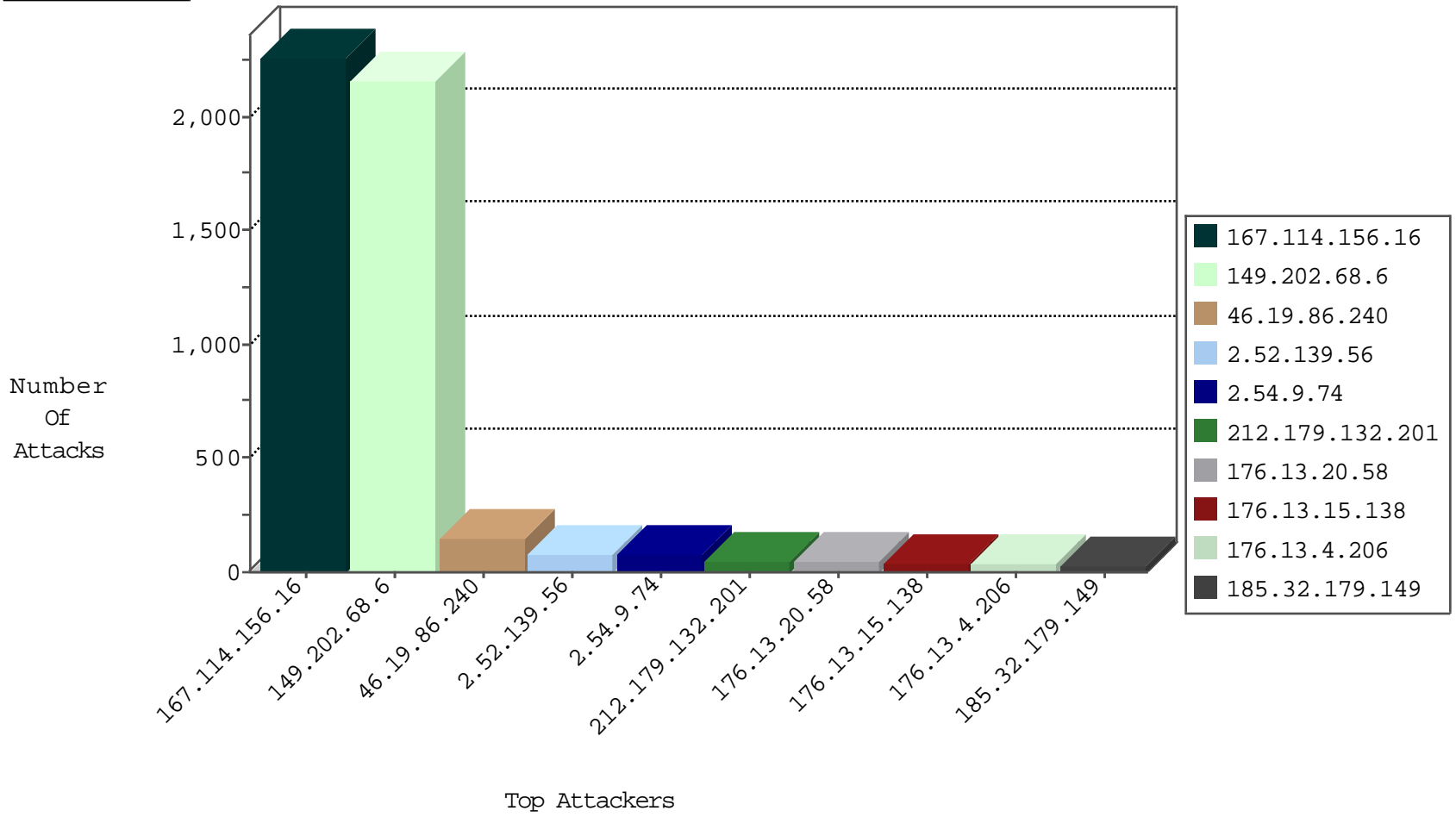
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3639
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
193.242.218.6	Switzerland	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
198.20.87.98	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
104.239.173.81		147.237.8.50	e.tikshuv.idf.il	Invalid I4 Header Length	drop	1
219.232.243.28	China	147.237.77.74	law.idf.il	Invalid I4 Header Length	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.44.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.46.41.119	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.12.78	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.156.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.12.78	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
31.154.19.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.13.21.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.210.187.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.9.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
94.102.48.194	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.144.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.176.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.195.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.146.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.121.14.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	784
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack		reject	593
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	454
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	227
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	71
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
212.179.132.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	32
176.13.15.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
2.54.9.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.9.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.9.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.54.9.74	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	12
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.197.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.9.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.54.9.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.214.104	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.185.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
95.35.164.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.30.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.65.185.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.132.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.60.90	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.23.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.140.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
194.114.146.227	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.84.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.179.132.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.199.57.197	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
46.19.85.159	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.30.24.97	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.0.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.146.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.219.119.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.102.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.8.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.55.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.133.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.41.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
2.52.139.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
176.13.20.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.4.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
185.32.179.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
149.202.239.135	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
2.52.143.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.1.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
109.65.215.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	4
82.166.53.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.31.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.76.118.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mailbox.aspx&sa=u&ved=0ahukewjm_73g_mt1ahv_gdw8khuhfdmkqfgglmaa&usg=afqjcnfw8xbjdj46aa_ieeng07gs79p8hq	Block	3
80.246.133.167	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.136.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.82.88	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.215.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.215.194	Block	2
185.32.179.149	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.35.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.150.215.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/112369.pdf	Block	2
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
61.5.70.36	Indonesia	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/209-he/patzar.aspx	Block	1
212.235.103.203	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.0.0.46	Jordan	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 141.0.0.46	Block	1
37.26.148.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.15.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
157.55.39.181	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.69.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106577.pdf	Block	1
213.204.106.26	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arabic/	Block	1
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/himush/site/he/himush.asp	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct171 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Malformed URL ũ•4™ @Ū";™[[ #30[[ ]]#16 ]]i[[#23]] h•	Block	1
61.5.70.36	Indonesia	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/801-he/patzar.aspx	Block	1
212.235.103.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.0.0.46	Jordan	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files	Block	1
84.108.105.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/daily_statistics/english/i.doc.(sources	Block	1
75.102.8.33	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
162.144.86.91	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/108847.pdf	Block	1
212.117.140.170	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
185.82.52.225		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.245.163.24	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1