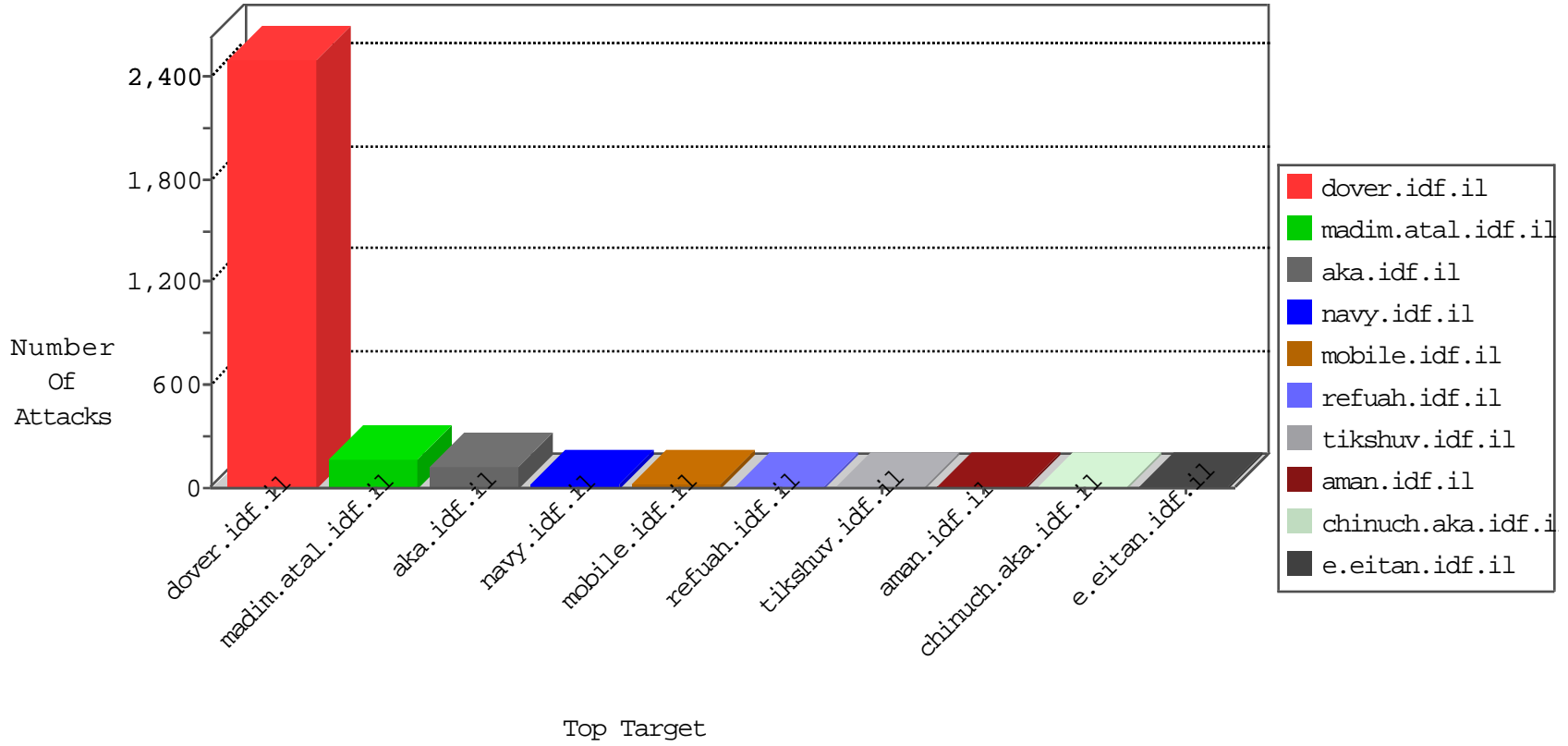


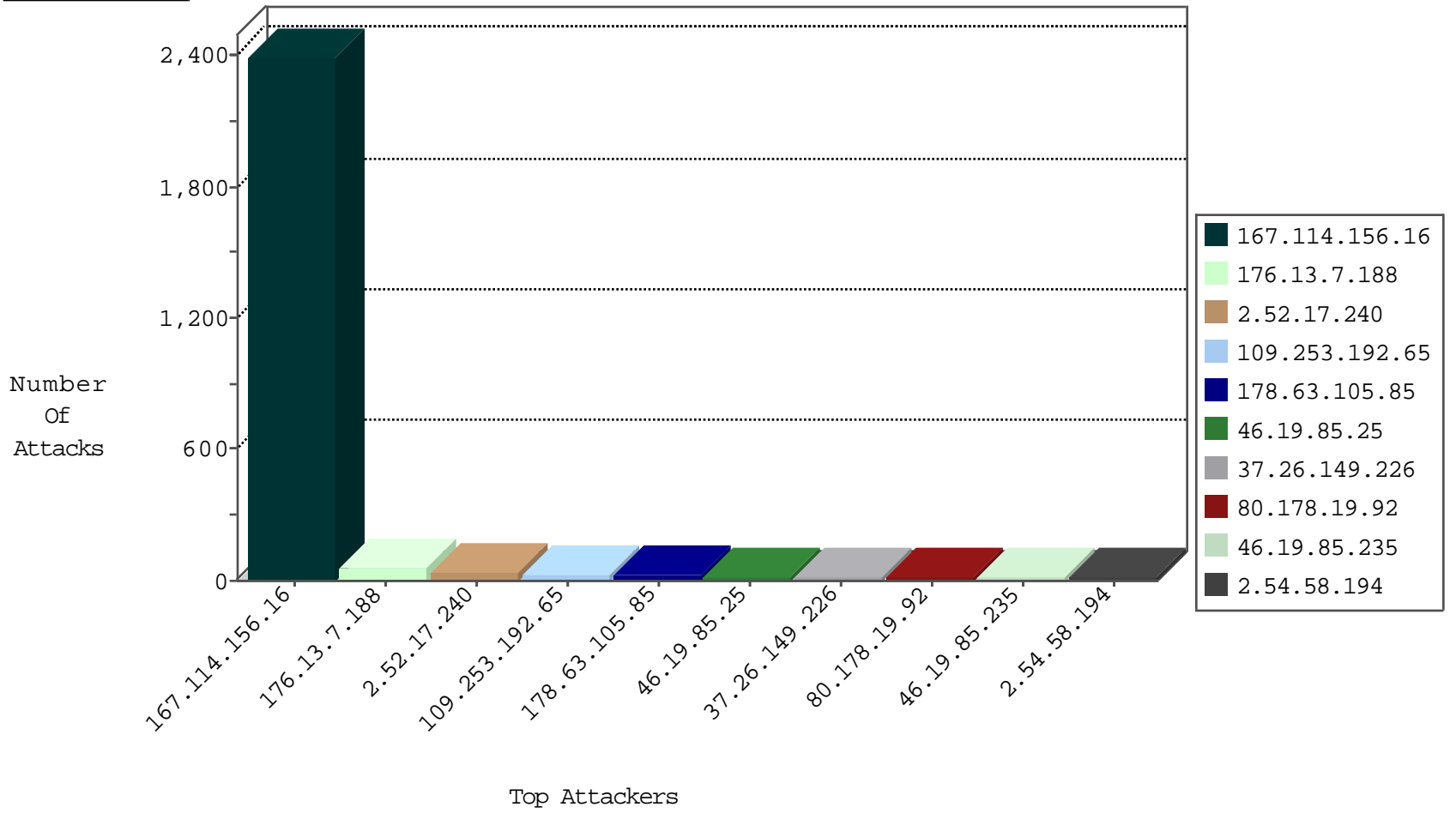
# IDF Under Attack Daily Report



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	3537
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.46.102.242	Romania	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.177.16.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.69	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
196.38.217.232	147.237.8.45	South Africa	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
185.72.179.221	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.185.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.17.218.231	147.237.77.176	Italy	matpash.idf.il	ET SCAN Potential SSH Scan	1
79.17.218.231	147.237.76.148	Italy	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
79.17.218.231	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.147	Cote D'Ivoire	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.38.217.232	147.237.8.45	South Africa	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
185.103.252.60	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.177.159.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.17.218.231	147.237.76.197	Italy	e.himsh.idf.il	ET SCAN Potential SSH Scan	1
79.17.218.231	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
2.52.17.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	10
109.65.37.99	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.17.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
197.134.127.64	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.17.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.17.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
209.126.230.71	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	5
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.23.34	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
109.64.49.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	4
46.19.85.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.139.238	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.199.251.227	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.17.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
173.36.240.168	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.85.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.10.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.55.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.70.87.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.116.243.196	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.149.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.14.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.170.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.103	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.23	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
80.178.19.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.95.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.139.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
62.0.34.177	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.137.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
85.64.247.71	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
79.180.137.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.7.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
109.253.192.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
37.26.149.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
2.54.58.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
80.178.19.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
213.8.204.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
95.86.113.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	3
37.26.149.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.178.157.105	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.70.96.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
80.184.44.156	Kuwait	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
37.26.147.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.211.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
68.180.230.189	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
209.126.230.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
157.55.39.46	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.144.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
74.201.226.103	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/16037.jpg	Block	1
64.233.172.238	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
74.201.226.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/displayallsoldiers.asp	Block	1
162.243.188.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1457395200030	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.142.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.32	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.126	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
185.3.144.51	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
84.95.251.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1