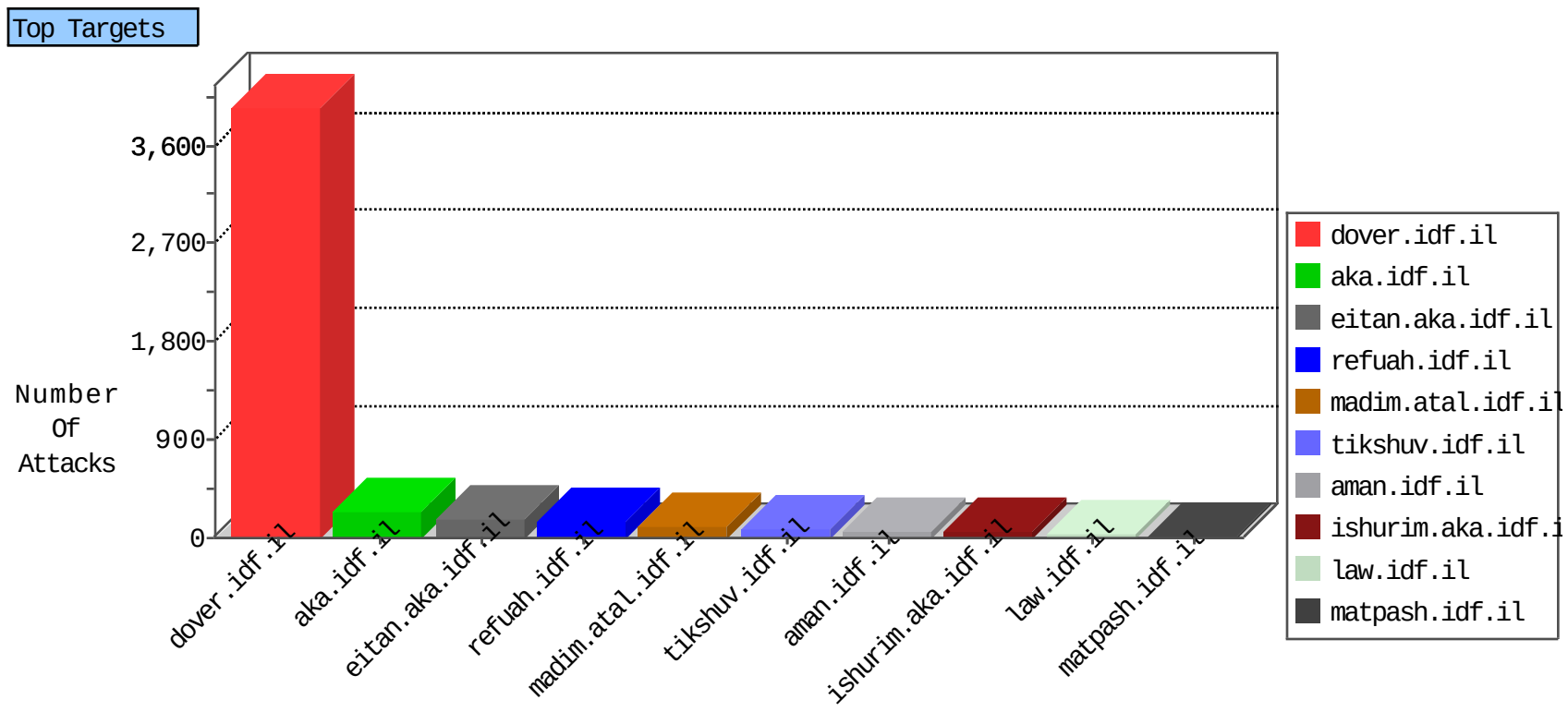
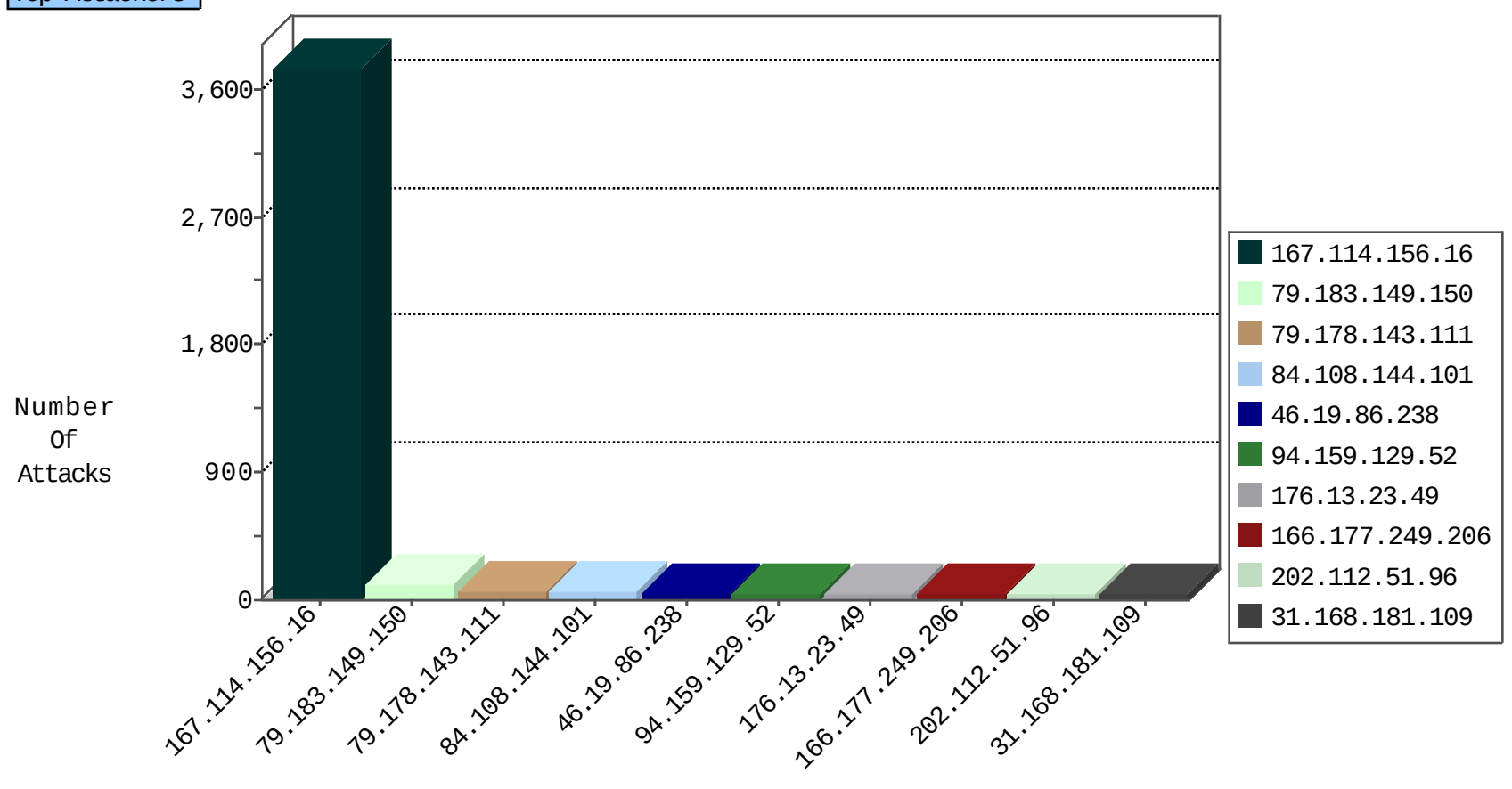
04-17-2016-18:04:02 to 04-17-2016-19:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-17-2016-18:04:02 to 04-17-2016-19:04:02

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	3756
84.108.144.101	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	8
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
202.112.51.96	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
202.112.51.96	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
182.200.20.247	China	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
111.227.26.175	China	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
66.240.219.146	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
122.84.162.51	China	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
212.179.247.58	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
192.96.201.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
212.179.247.58	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1

04-17-2016-18:04:02 to 04-17-2016-19:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.165.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.57.205.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.109.180.213	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
84.109.180.213	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
84.109.180.213	Israel	147.237.77.176	matpash.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
68.64.168.226	United States	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
151.80.31.108	France	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

04-17-2016-18:04:02 to 04-17-2016-19:04:02

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	3
86.190.61.232	147.237.0.33	United Kingdom	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.232.207.210	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.178	Latvia	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
62.232.207.210	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
62.232.207.210	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
169.1.165.42	147.237.77.216	South Africa	dover.idf.il	portscan: TCP Distributed Portscan	1
40.114.42.13	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
149.50.124.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.246.145	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.170.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.245.177	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
217.133.53.77	147.237.76.86	Italy	navy.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.14.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.77.179	Latvia	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
62.232.207.210	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
195.154.54.169	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.232.207.210	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.70.184.206	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
62.210.142.238	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.48.204	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.223.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.1.167.240	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.245.177	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.65.250.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.35.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -f -sS	1

04-17-2016-18:04:02 to 04-17-2016-19:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.149.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
79.178.143.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
94.159.129.52	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
84.108.144.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
31.168.181.109	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.23.49	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.137	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.8.2.85	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	20
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
166.177.249.206	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.55.51.113	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.156.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
166.177.249.206	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
80.246.130.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
84.111.37.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.23.49	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.97.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.66.175	Israel	147.237.0.34	tikshuv.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	6
37.26.149.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.194.199.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.234.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.239.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
166.177.249.206	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.144.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
166.177.249.206	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.165.81	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.242.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.129.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.62.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.41.5	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.116.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	4
77.127.67.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.191.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.181.243.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.13.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.161.199	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
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.194.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
89.139.152.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
41.47.175.217	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.6.57.114	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
41.47.245.90	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.154.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.209.5	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
2.53.166.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.248	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
197.199.207.9	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
45.63.105.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/wp-login.php	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brohers/home/default.aspx	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
180.76.15.12	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-he/refuah.aspx	Block	1
78.188.169.77	Turkey	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
202.112.51.96	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to bter.com/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main_index.stm.	Block	1
79.179.177.209	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/ge	Block	1
207.232.46.209	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.144.33	Block	1
95.35.38.2	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
79.177.104.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gen204	Block	1
202.112.51.96	China	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to bter.com/	Block	1
2.53.171.127	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
141.212.122.81	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /x	Block	1
80.246.130.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8919-he/refuah.aspx	Block	1
213.8.204.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
41.47.236.108	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.143.179	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
202.112.51.96	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to bter.com/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
5.29.164.247	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
149.88.166.197	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.144.101	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
216.72.34.205	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
79.178.143.111	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.62	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9738-he/refuah.aspx	Block	1
31.210.187.140	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter id in aka.idf.il/main/giyus/login.aspx	None	1
89.139.62.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1