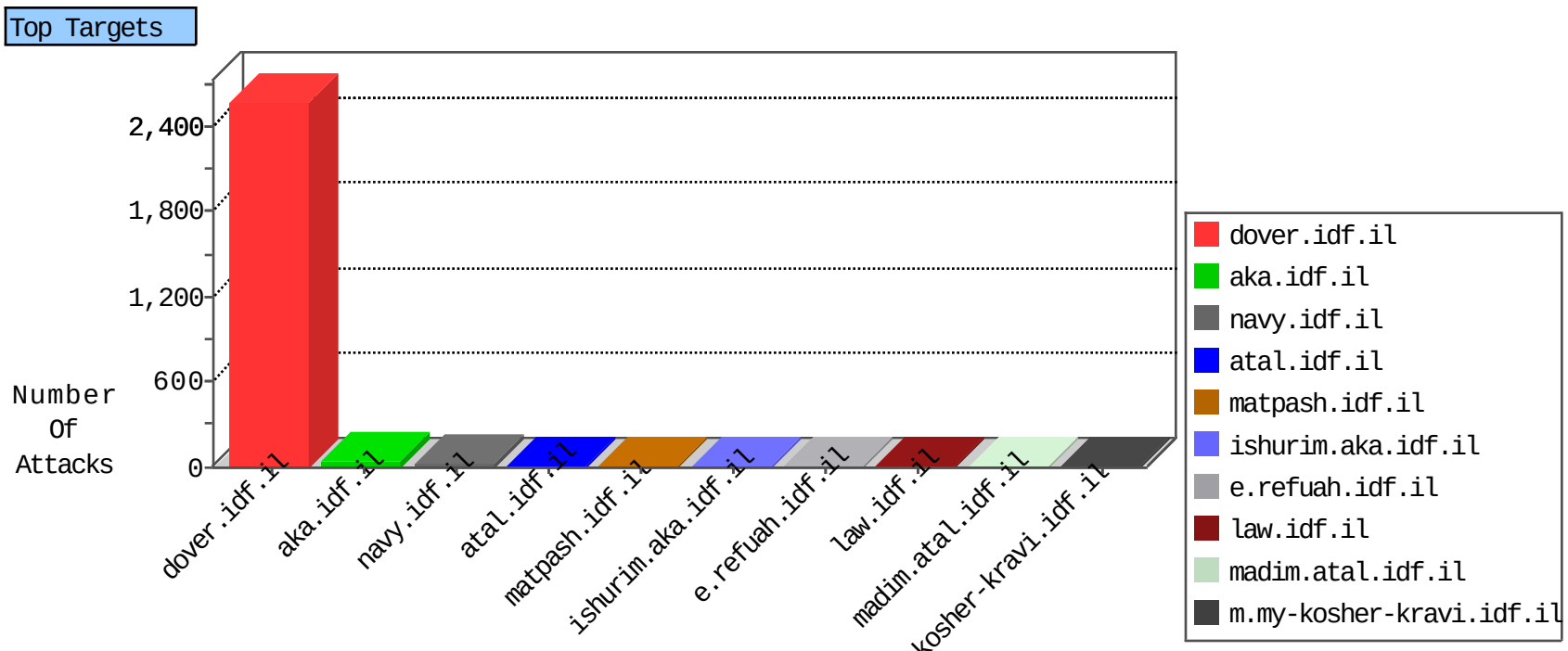
01-24-2016-05:04:08 to 01-24-2016-06:04:08

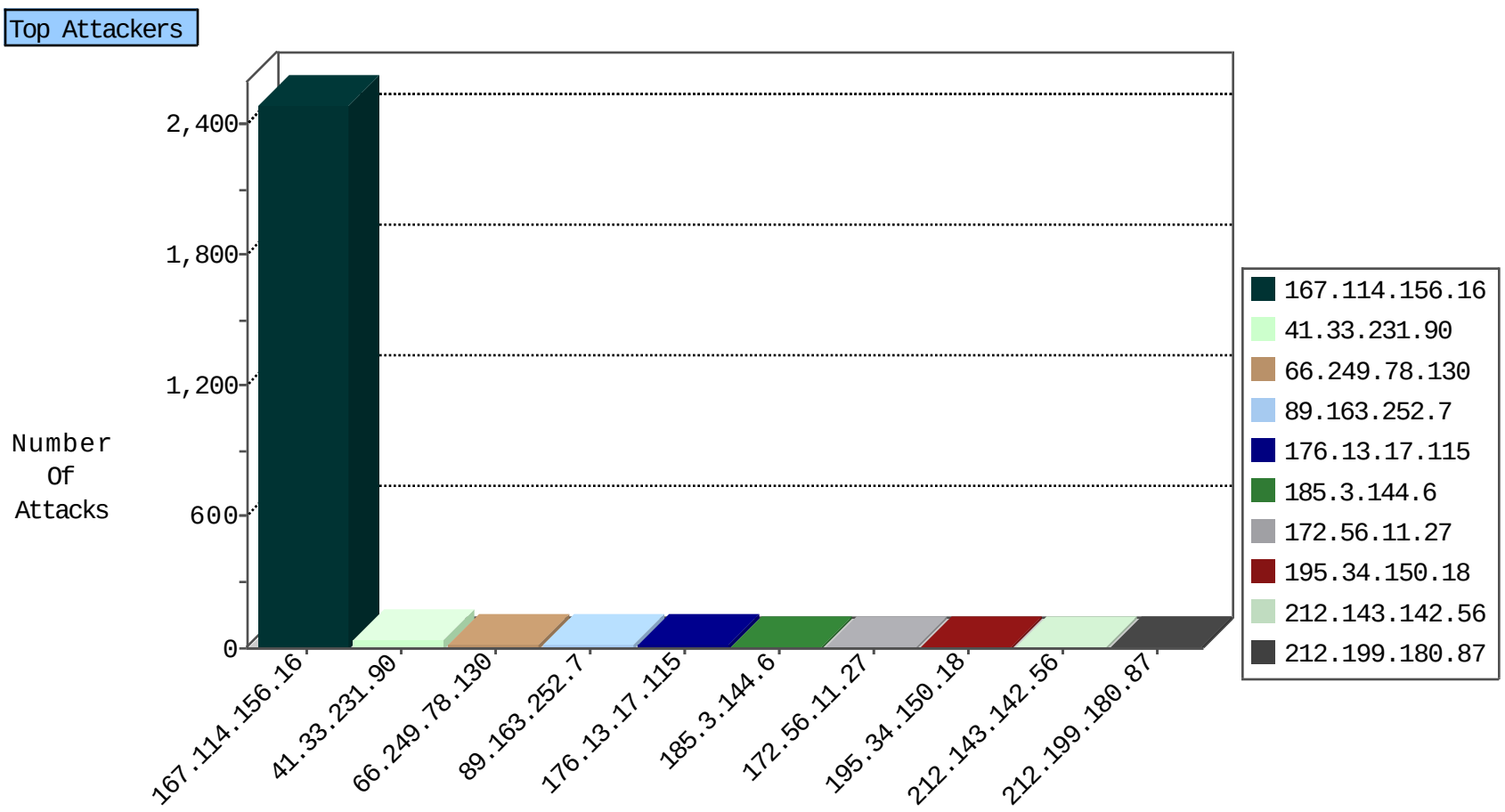
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-24-2016-05:04:08 to 01-24-2016-06:04:08

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	3127
50.135.11.137	United States	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	4
115.239.228.10	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-24-2016-05:04:08 to 01-24-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
136.243.5.215	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
185.66.249.87	Netherlands	147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

01-24-2016-05:04:08 to 01-24-2016-06:04:08

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	4
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
89.163.252.7	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.121	Kazakstan	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
125.65.165.215	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.252.7	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
182.131.21.69	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.0.200	Germany	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.13.17.115	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
89.163.252.7	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.77.121	Kazakstan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
89.163.252.7	147.237.77.234	Germany	halag.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
89.163.252.7	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.252.7	147.237.72.217	Germany	e.idf.il	ET SCAN Potential SSH Scan	1
183.1.72.137	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.163.252.7	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
182.131.21.69	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-24-2016-05:04:08 to 01-24-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.199.180.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.11.27	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
176.13.17.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
193.90.12.86	Norway	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.17.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
97.46.131.138	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.56.11.27	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
208.83.215.176	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
94.230.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.40	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.144.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.76.15.11	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
198.1.101.123	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.116	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.186.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.76.15.11	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
104.156.240.200	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.119	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.192	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
180.76.15.147	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
172.56.11.27	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.232.110.28	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
204.79.180.181	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
74.82.47.16	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.144.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

01-24-2016-05:04:08 to 01-24-2016-06:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.212.121.192	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
222.186.56.107	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.229.230	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
180.76.15.155	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
94.23.54.167	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20792-he/dover.aspx.	Block	1
5.29.60.11	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.253.198.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
185.3.144.6	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
95.86.65.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21198-he/dover.aspx&sa=u&ved=0ahukewi5_cxuwshkahuhzrqkhbyyaisqfgghmac&usg=afqjcnhp-hai-kejcabnayloeopevqbdgq	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
37.59.123.142	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
159.203.86.106	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/228-he/faq.aspx	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
185.20.4.143	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
95.86.110.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/manilot/	Block	1
40.77.167.45	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
159.203.86.106	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
50.63.8.35	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1