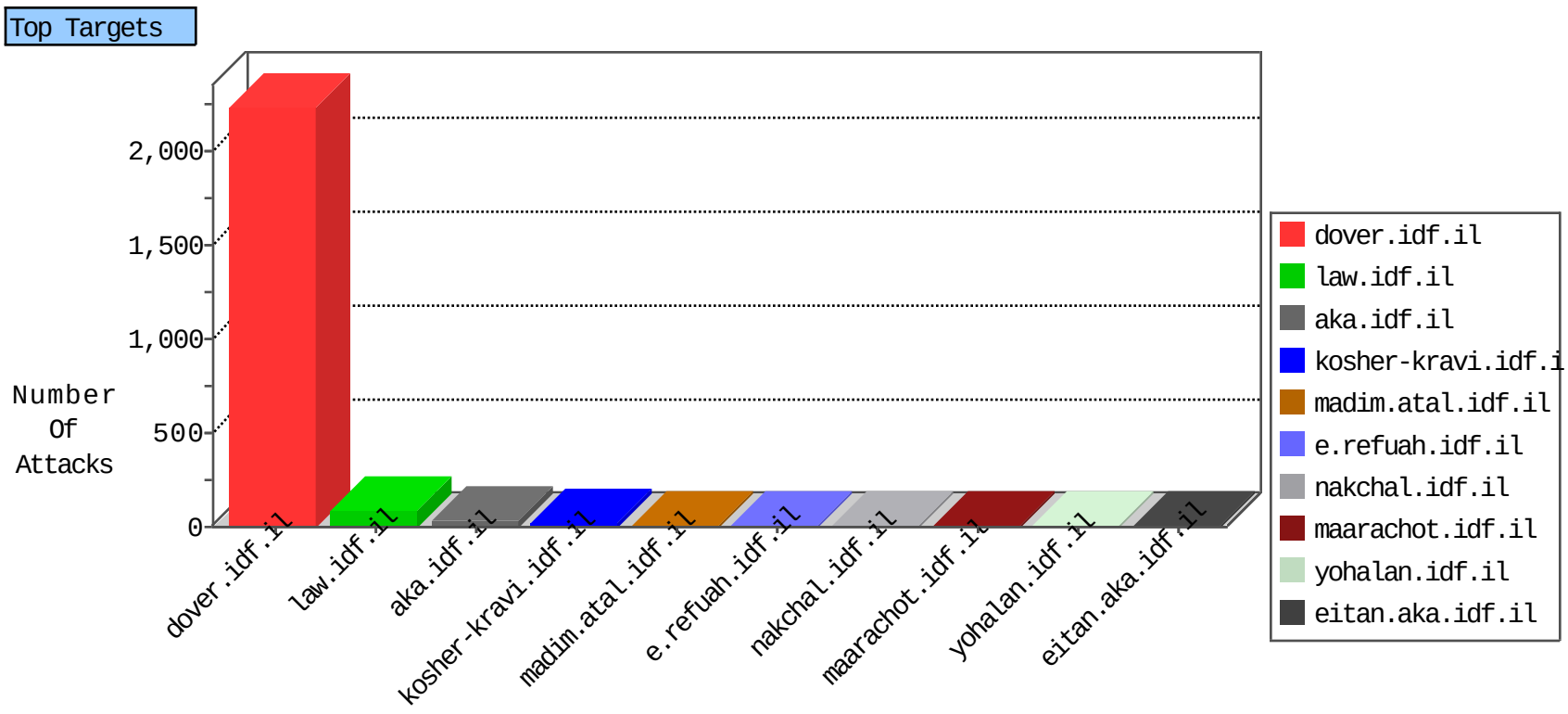
12-18-2015-04:04:00 to 12-18-2015-05:04:00

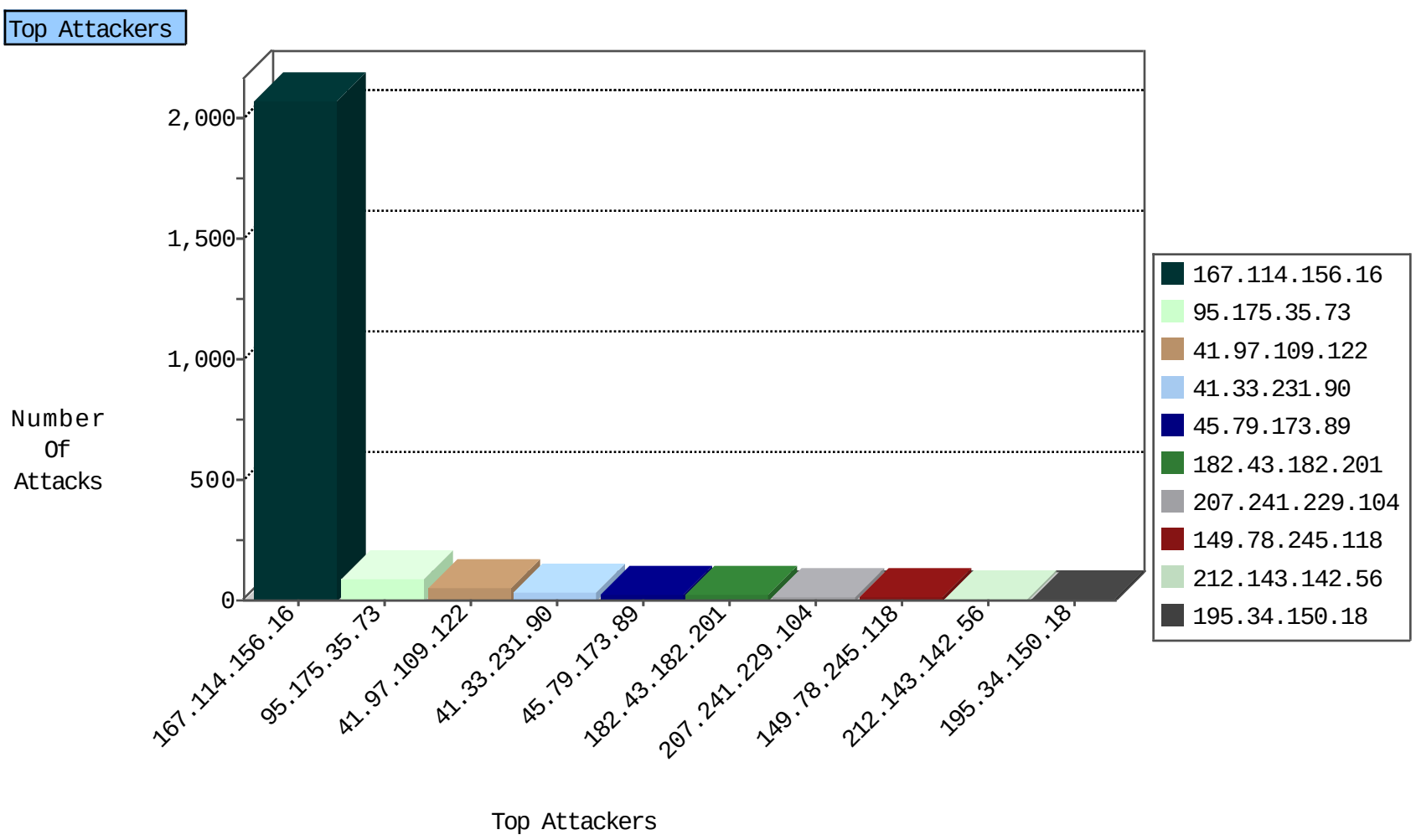
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-18-2015-04:04:00 to 12-18-2015-05:04:00

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	3409
113.10.136.95	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
115.231.222.40	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
115.231.222.40	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

12-18-2015-04:04:00 to 12-18-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
78.46.174.197	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-18-2015-04:04:00 to 12-18-2015-05:04:00

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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.46.193.114	147.237.77.235	China	sviva.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.77.235	China	sviva.idf.il	GPL SCAN nmap TCP	2
182.43.182.201	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
182.43.182.201	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
182.43.182.201	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
182.43.182.201	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
124.119.78.119	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.43.182.201	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
182.43.182.201	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
182.43.182.201	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.43.182.201	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -f -sS	1
199.191.56.188	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
182.43.182.201	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.188	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -f -sS	1
182.43.182.201	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
182.43.182.201	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
124.219.49.98	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
182.43.182.201	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
182.43.182.201	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.70.45.51	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.43.182.201	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
58.253.96.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
182.43.182.201	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
212.7.211.7	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.173.89	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
182.43.182.201	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.188	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
182.43.182.201	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1

12-18-2015-04:04:00 to 12-18-2015-05:04:00

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
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	drop		drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.148.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
76.104.48.153	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.185.165.250	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.185.165.250	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.141.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
76.16.133.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
76.16.133.174	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
5.175.26.46	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
89.207.130.134	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.227.69	Anonymous Proxy	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
92.222.242.103	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.223	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.65.120.48		147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.119	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.121.191	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.94	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.14	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.127	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
58.97.36.46	Thailand	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.96	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
92.222.242.103	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.65.120.48		147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.119	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.65	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.116	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.26	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.221	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
61.135.190.72	China	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.111	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.122	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.65.120.48		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.120	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.175.35.73	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 95.175.35.73	Block	86
41.97.109.122	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.97.109.122	Block	46
149.78.245.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
31.131.16.162	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.131.16.162	Block	5
85.64.92.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
41.97.109.122	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-ar/dover.aspx	Block	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
2.54.35.35	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.75.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/rights/asp/info.asp	None	1
66.249.66.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1097-he/nakhal.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
131.253.25.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/i/jot	Block	1
5.175.26.46	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.75.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
88.231.222.38	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
141.212.122.112	United States	147.237.77.170	maarachot.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
45.79.173.89		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
197.162.98.99	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
207.46.13.128	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/×’ Ö³Ã¯Ö²Â¿Ö²Â½Ö³Ã¯Ö²Â¿Ö²Â½	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
141.212.122.112	United States	147.237.77.233	atal.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
31.131.16.162	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1966-he/cogat.aspx	Block	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1085-he/nakhal.aspx	Block	1
66.249.66.21	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1071-he/nakhal.aspx	Block	1
197.162.98.99	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/i/js_inst	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17900-en/dover.aspxyou	Block	1
146.185.234.48	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	1
40.77.167.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ca0qfjaaahukewij6_kykpfgahwjxhqkhvtgdnu&sig2=ndaz6msozbm1ftpnczrgha&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
74.82.47.4	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
66.249.66.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1122-he/nakhal.aspx	Block	1
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1