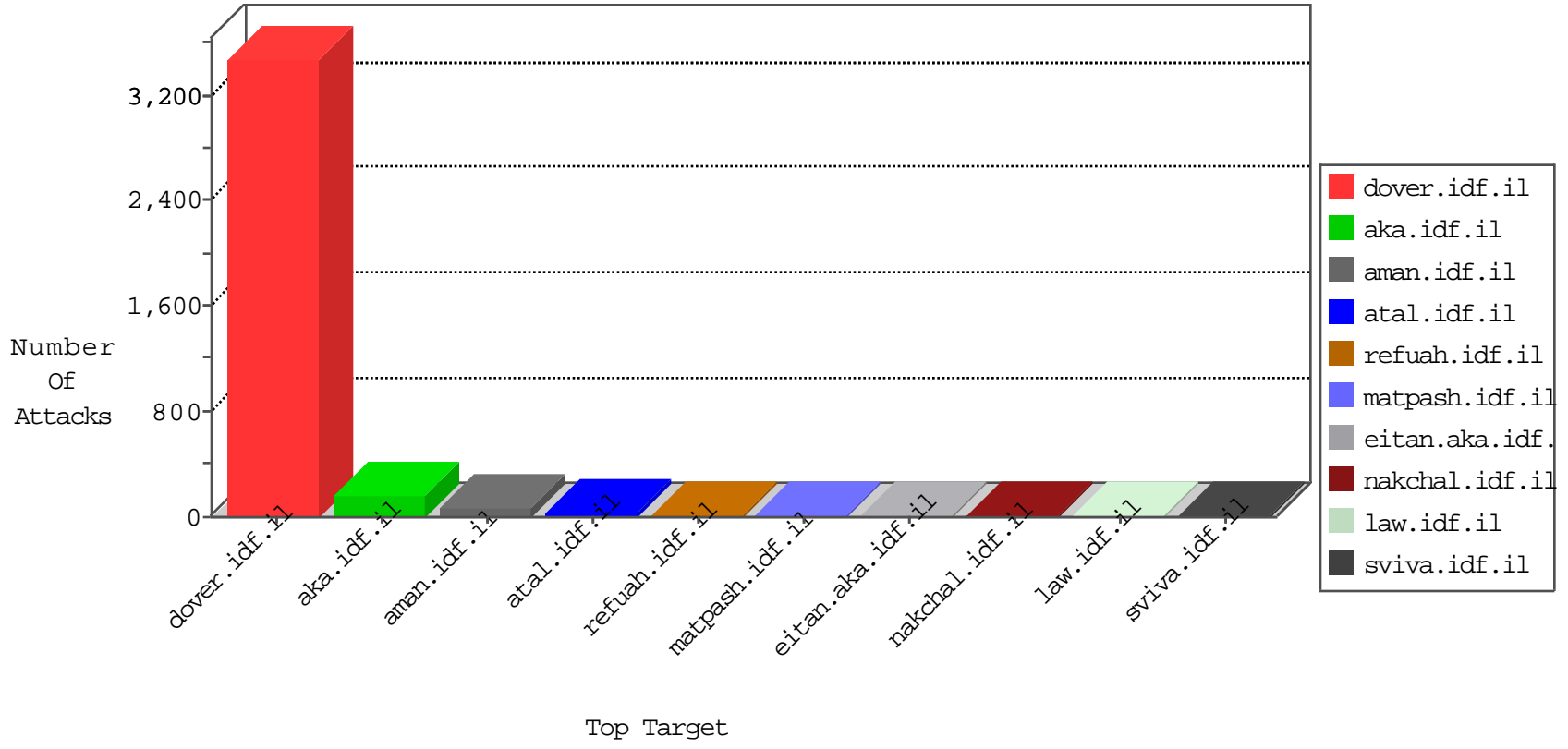


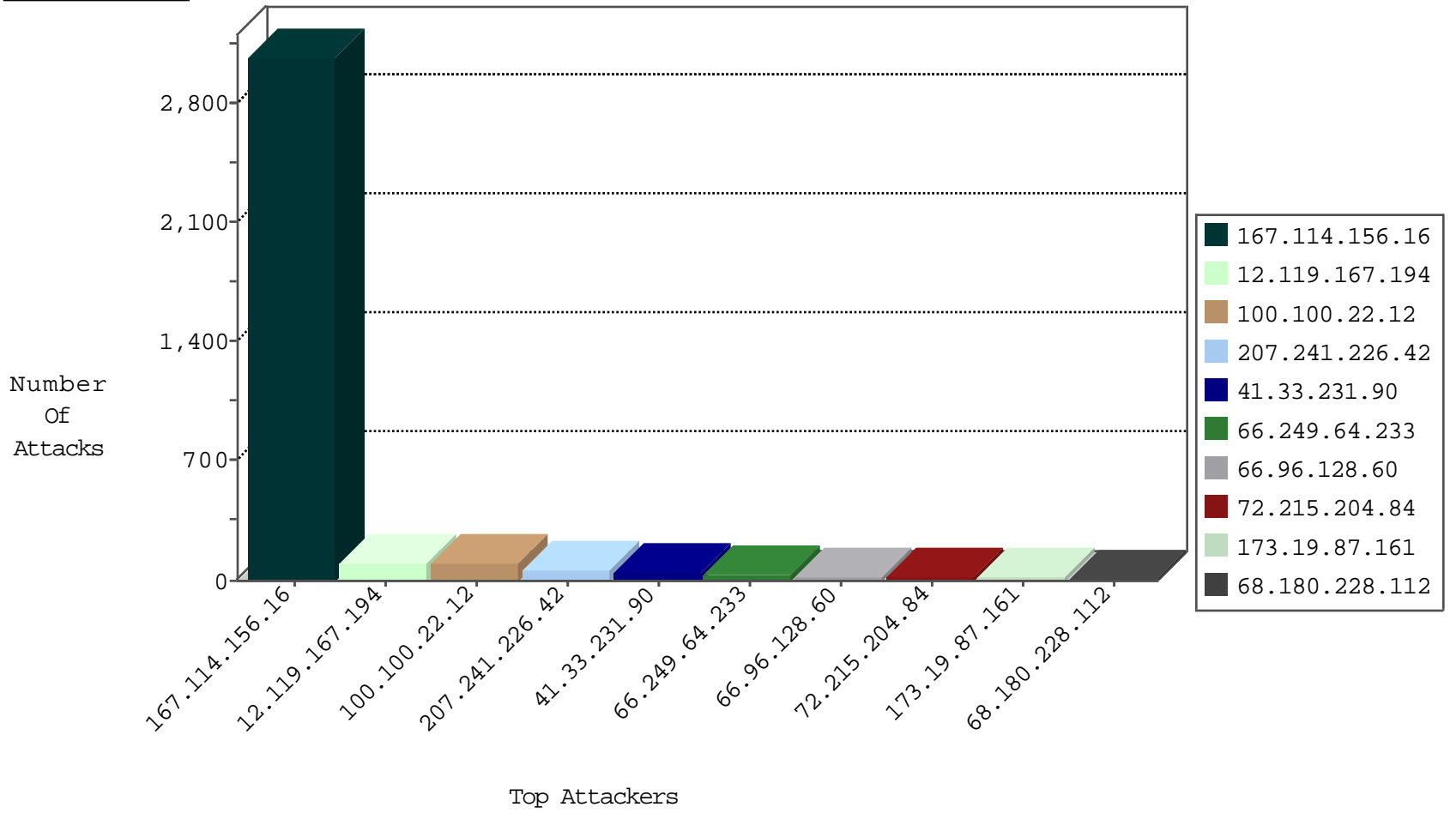
IDF Under Attack Daily Report



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	3096
113.240.234.245	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-25-2015-03:04:08 to 11-25-2015-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.65.37	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.82	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.98	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
31.6.71.154	147.237.77.235	Poland	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
23.227.196.29	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
23.227.196.29	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
220.225.147.173	147.237.0.33	India	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.19.138.144	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.6.71.154	147.237.77.176	Poland	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
23.227.196.29	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
166.149.26.62	147.237.72.14	United States	dover.idf.il(old	ET SCAN Potential SSH Scan	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	drop	First packet isn't SYN	drop	830
12.119.167.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
100.100.22.12		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	61
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
100.100.22.12		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
72.215.204.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
95.175.97.229	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.203.98.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
173.19.87.161	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
119.137.66.131	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
197.6.131.164	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.124	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.185.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
69.171.228.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
173.19.87.161	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
86.108.32.221	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
204.79.180.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
173.19.87.161	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
207.241.226.42	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	3
66.249.64.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.93.18.64	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.241.226.42	United States	147.237.72.166	aka.idf.il	drop		drop	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.171.228.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
99.237.141.6	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.10.104.243	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.66.118	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.241.226.42	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.7.124.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
204.79.180.130	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.171.228.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	57
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.137.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.244	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18762-he/dover.aspx	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
213.193.11.206	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.126.102.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/sfinathamidbar.aspx	Block	1
197.36.235.41	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.142.68.105	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
137.122.64.31	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.176.60.161	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
176.12.143.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
5.29.54.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.193.11.206	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
79.176.60.161	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
207.241.226.42	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
37.142.68.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
141.212.122.160	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
79.176.60.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
197.36.189.186	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
5.29.234.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.60.161	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
157.55.39.124	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.214.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
197.36.189.186	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3259.jpg	Block	1
119.137.66.131	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
79.176.60.161	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/opennativkalandia.aspx	Block	1
207.241.226.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/msxml2.xmlhttp	Block	1
157.55.39.124	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19478-he/idfgdover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1