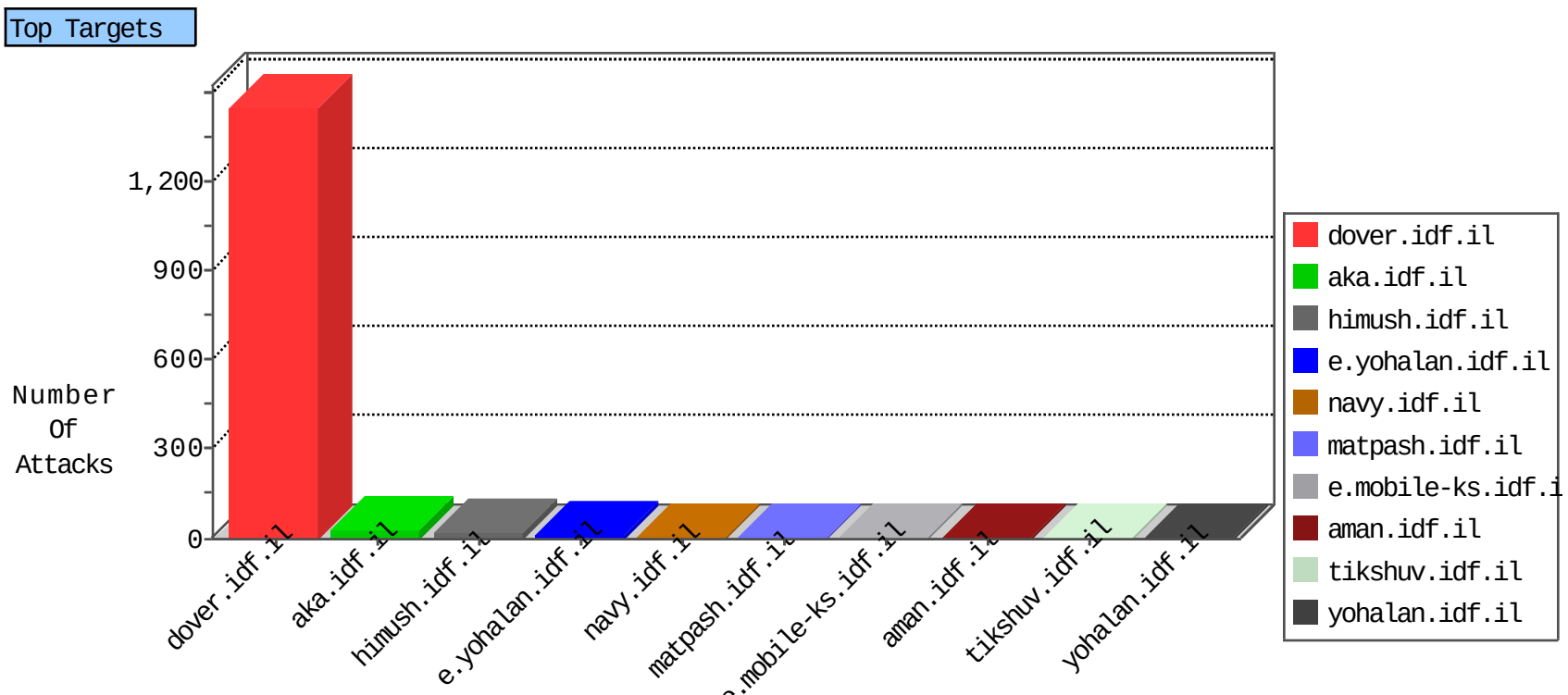
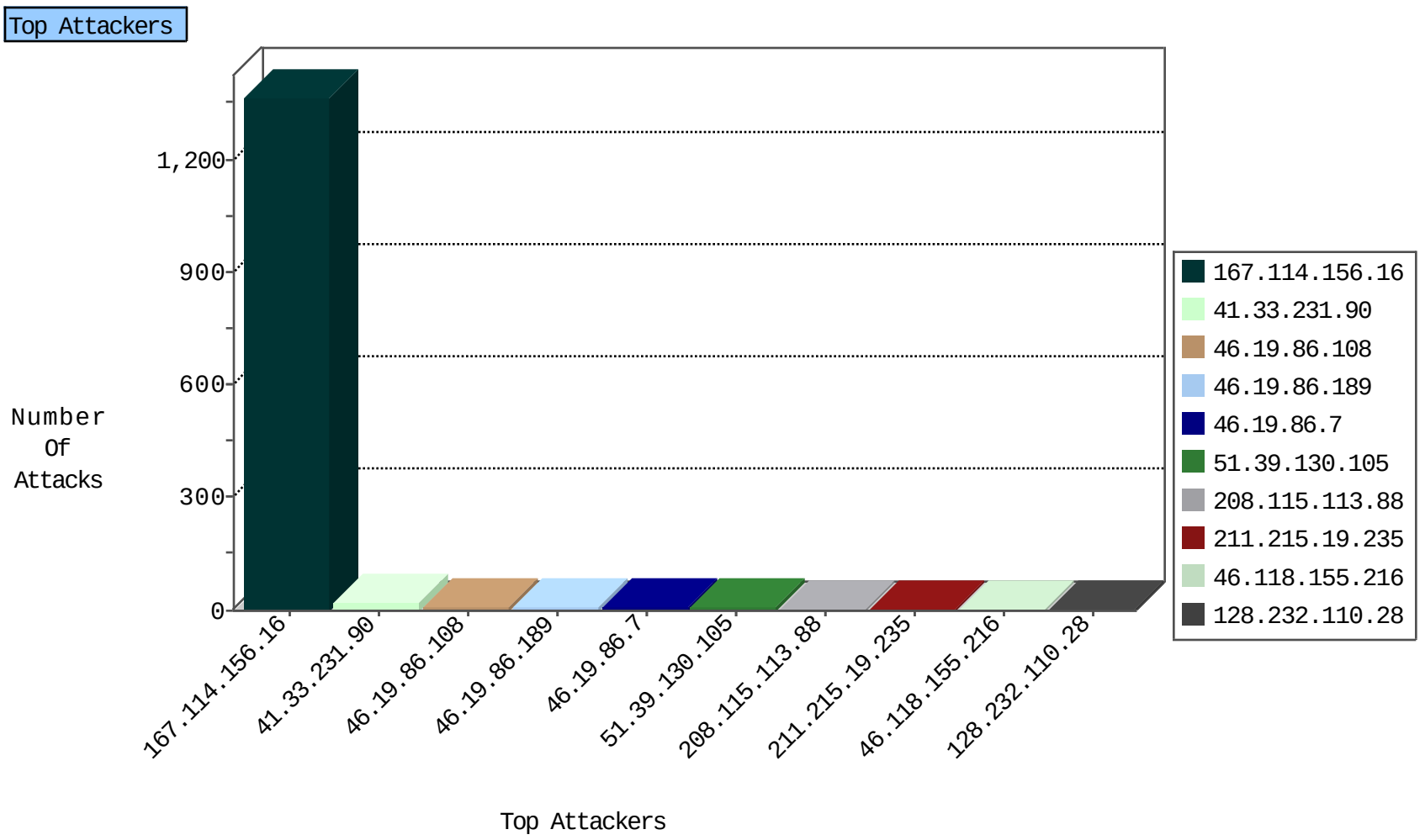
12-15-2015-05:04:04 to 12-15-2015-06:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-15-2015-05:04:04 to 12-15-2015-06:04:04

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	3539

12-15-2015-05:04:04 to 12-15-2015-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.49.56	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1

12-15-2015-05:04:04 to 12-15-2015-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
82.211.60.82	147.237.76.34	Germany	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
218.205.129.146	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
78.193.2.8	147.237.0.35	France	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.149.252.58	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
211.215.19.235	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.149.252.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
211.215.19.235	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.50.100.130	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
182.72.109.162	147.237.77.179	India	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.148.30.199	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.10.114.32	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 4096	1
39.67.49.112	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.96.254.231	147.237.77.212	Romania	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
36.110.44.178	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
82.211.60.82	147.237.76.34	Germany	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.143.163	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
82.211.60.82	147.237.76.34	Germany	yohalan.idf.il	ET SCAN NMAP -f -sS	1
218.205.129.146	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
211.215.19.235	147.237.76.39	Korea, Republic of	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
61.149.252.58	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
211.215.19.235	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.149.252.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
61.50.100.130	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.37	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 3072	1
36.110.44.178	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.113	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
23.97.172.218	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

12-15-2015-05:04:04 to 12-15-2015-06:04:04

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	12
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.9	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
77.125.126.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.121.188	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.178	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.160.233.254	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.59.159.58	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.79	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.76	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.183	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.196.104.39	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.231.6.246	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.20	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.120	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.191	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
32.218.140.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.179	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
122.53.132.114	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.185	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.196.104.39	China	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.231.6.246	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
74.82.47.58	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.208	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.64	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.181	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.94	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.116.97.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.186	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.196.104.39	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.70	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
42.62.74.71	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.182	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.100	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.187	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-15-2015-05:04:04 to 12-15-2015-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
176.13.14.31	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
51.39.130.105	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
149.88.92.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.115.111.74	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.44	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
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	2
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
51.39.130.105	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 51.39.130.105	Block	2
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	2
175.197.148.112	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.197.148.112	Block	2
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.59.148.210	Block	1
52.70.244.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13421-en/dover.aspx/	Block	1
175.197.148.112	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/{1}	Block	1
118.159.230.98	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
68.180.229.27	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17672.jpg	Block	1
157.55.39.3	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	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
54.209.172.211	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.108	Block	1
139.196.104.39	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2061-he/cogat.aspx	Block	1
157.55.39.8	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	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
208.115.113.93	United States	147.237.76.30	himush.idf.il	Suspicious Response Code	Block	1
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
180.76.15.10	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
141.8.142.24	Russian Federation	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.46.13.168	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/109335.pdf×•Â»Â¢×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»-×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»×•Â»Â¢×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
108.26.200.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
180.76.15.142	China	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.64	United States	147.237.77.19	law-forum.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
51.39.130.105	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login.php	Block	1
109.67.209.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1

12-15-2015-05:04:04 to 12-15-2015-06:04:04