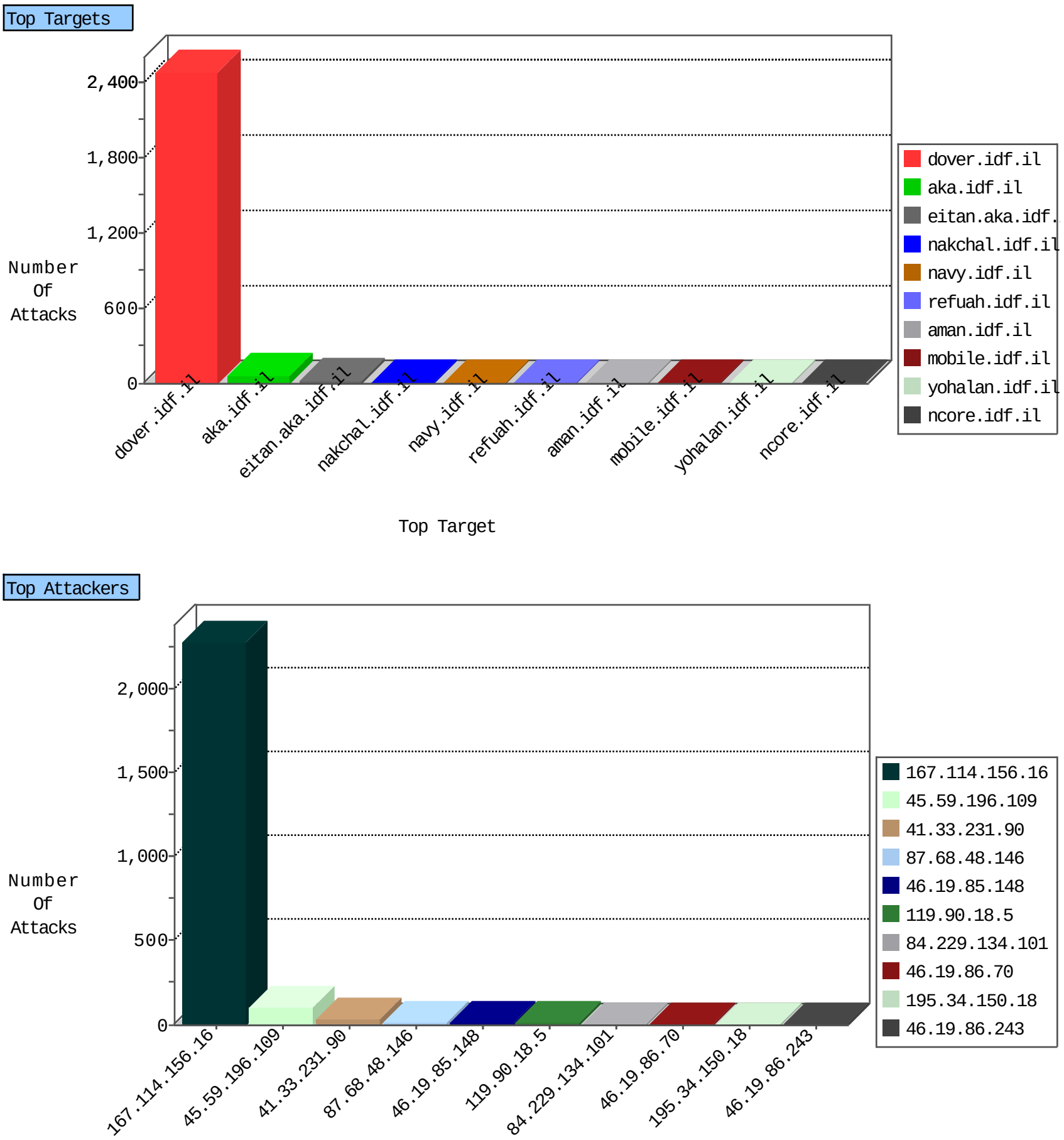
12-22-2015-01:07:43 to 12-22-2015-02:07:43

IDF Under Attack
Daily Report



12-22-2015-01:07:43 to 12-22-2015-02:07:43

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	3135
178.162.198.135	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
177.235.236.180	Brazil	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
177.235.236.180	Brazil	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-22-2015-01:07:43 to 12-22-2015-02:07:43

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.59.196.109		147.237.77.216	dover.idf.i	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
45.59.196.109		147.237.77.216	dover.idf.i	0854: HTTP: upload* Access	Block	12
185.63.188.120	Russian Federation	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
51.254.97.219	United Kingdom	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-22-2015-01:07:43 to 12-22-2015-02:07:43

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
66.249.64.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
208.80.155.223	147.237.76.200	United States	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	2
119.90.18.5	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.18.5	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
169.54.244.82	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -f -sS	1
119.90.18.5	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
51.254.44.137	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
172.245.11.57	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
119.90.18.5	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
119.90.18.5	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.238	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
168.62.238.153	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.18.5	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
119.90.18.5	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
178.20.72.19	147.237.76.31	Italy	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.18.5	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
172.245.11.57	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 3072	1

12-22-2015-01:07:43 to 12-22-2015-02:07:43

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.59.196.109		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
87.68.48.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.229.134.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.253	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.75.101	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.59.196.109		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.243	Israel	147.237.76.42	refuah.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
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.59.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.182.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.187.150.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.89.217.231		147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.17.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.101	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.146.111	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.180	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.231		147.237.76.31	nakchal.idf.il	Directory Traversal	directory traversal overflow	monitor	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
37.26.149.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.233		147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
137.116.71.170	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.246.187.42	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.2.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.89.217.234		147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.129.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.138.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.89.217.226		147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.175.193.232	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.26.149.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-22-2015-01:07:43 to 12-22-2015-02:07:43

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.59.196.109		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.59.196.109	Block	3
194.180.84.134	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.180.84.134	Block	2
45.59.196.109		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
199.30.25.101	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.23.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
149.88.31.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
31.154.144.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
176.67.201.86		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.76.247.204	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
46.19.86.140	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
157.55.2.171	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
208.80.155.223	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
180.76.15.146	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
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	1
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
194.180.84.134	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1640.jpg	Block	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18058-en/dover.aspx <a href=	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.8.128.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
183.206.167.34	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/js/fckeditor/editor/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.253	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1086-en/hamaz.aspx	Block	1
66.249.79.119	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1771	Block	1
45.59.196.109		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
185.89.217.231		147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	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

12-22-2015-01:07:43 to 12-22-2015-02:07:43