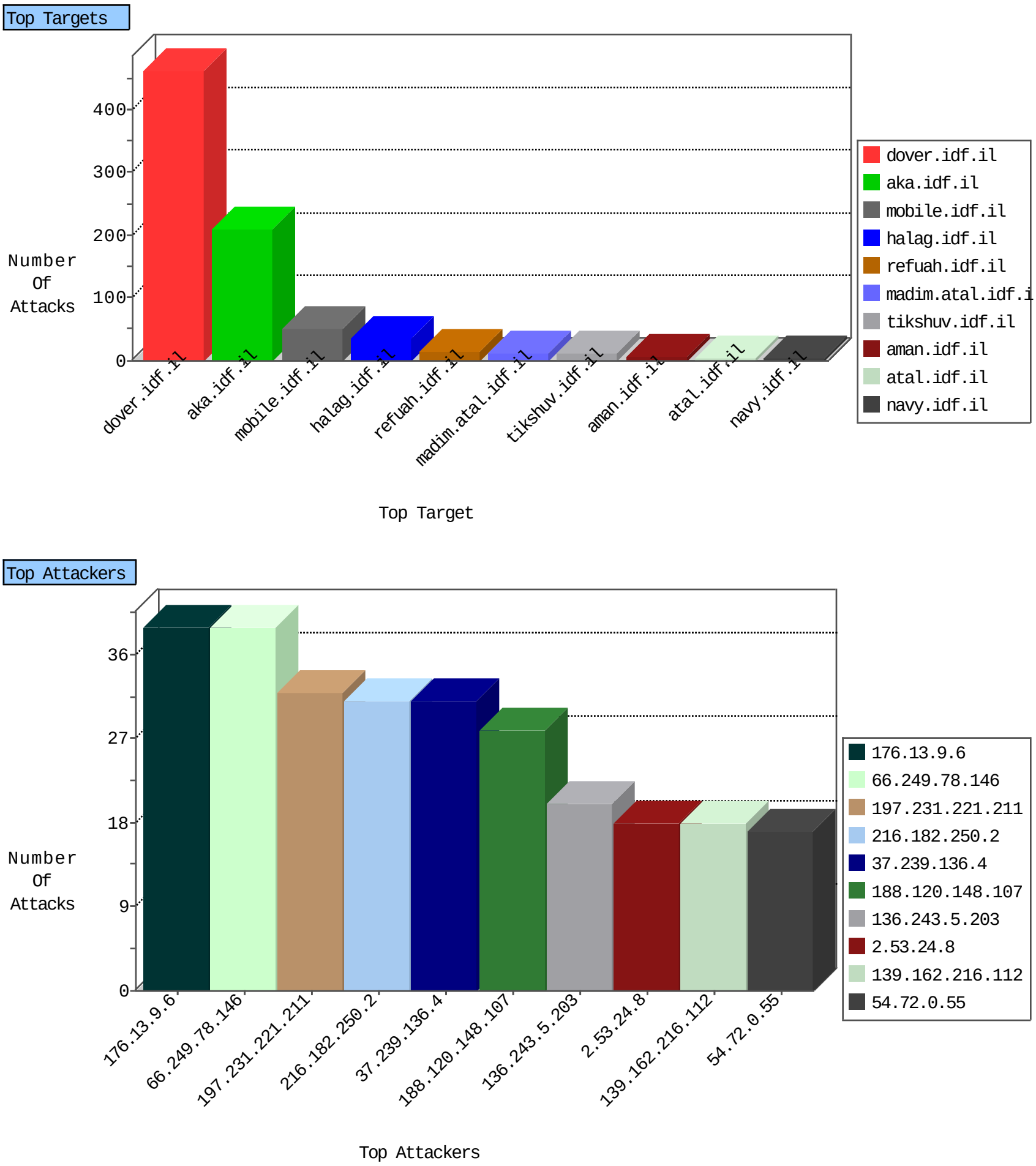
04-28-2016-22:04:03 to 04-28-2016-23:04:03

IDF Under Attack
Daily Report



04-28-2016-22:04:03 to 04-28-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.101.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3056
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
176.31.60.249	France	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
80.82.70.231	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
80.82.70.231	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

04-28-2016-22:04:03 to 04-28-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-22:04:03 to 04-28-2016-23:04:03

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	3
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.158	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
201.173.93.25	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.167.131	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.77.227	Lithuania	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
171.106.48.63	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
171.106.48.63	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
223.4.174.30	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.77.170	Lithuania	maarachot.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
171.106.48.63	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
95.173.184.12	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN Potential SSH Scan	1

04-28-2016-22:04:03 to 04-28-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
216.182.250.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
37.239.136.4	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
176.13.9.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
188.120.148.107	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.53.24.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
199.253.177.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.253.226.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.149.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
8.39.217.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.24.181.134	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.9.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.157.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.184	United States	147.237.0.34	tikshuv.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.94.199.16	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.89.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.43.218.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.163.67.14	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.162.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.82.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.189	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.44.112.87	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.98.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.146.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.196.97.44	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
93.83.206.50	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
130.253.27.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.58.158.109	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.131.72.120	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.108.98.60	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	5
199.30.25.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
199.30.24.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.157.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.119.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
199.30.25.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.58.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
38.88.199.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
65.55.210.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.157.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
87.139.236.153	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/broadweb/bwroot.asp	Block	1
66.249.66.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
14.114.25.226	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/phpsso_server/index.php	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.108.98.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.16.199	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
2.53.9.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
188.120.148.107	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.3.144.122	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.188	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
37.146.127.18	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx„'ƒ¨„,„¿„,„½„'•'ƒ¨„,„¿„,„½„'ƒ¨	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
2.53.19.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.25.69.18	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.212.122.161	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
87.70.75.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.59.202	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
212.25.69.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.212.122.161	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
87.139.236.153	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/broadweb/bwroot.asp	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
14.114.25.226	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1

04-28-2016-22:04:03 to 04-28-2016-23:04:03