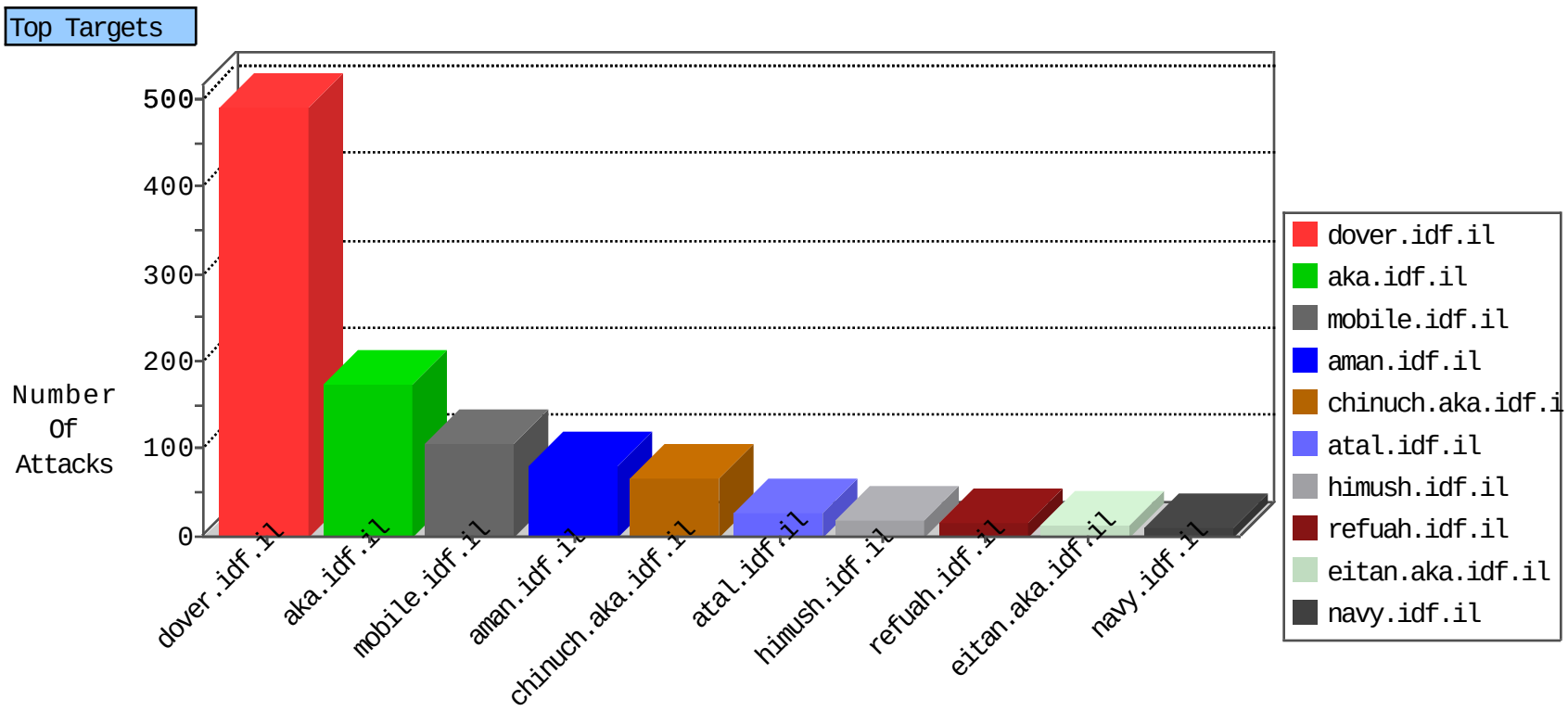
04-28-2016-01:04:12 to 04-28-2016-02:04:12

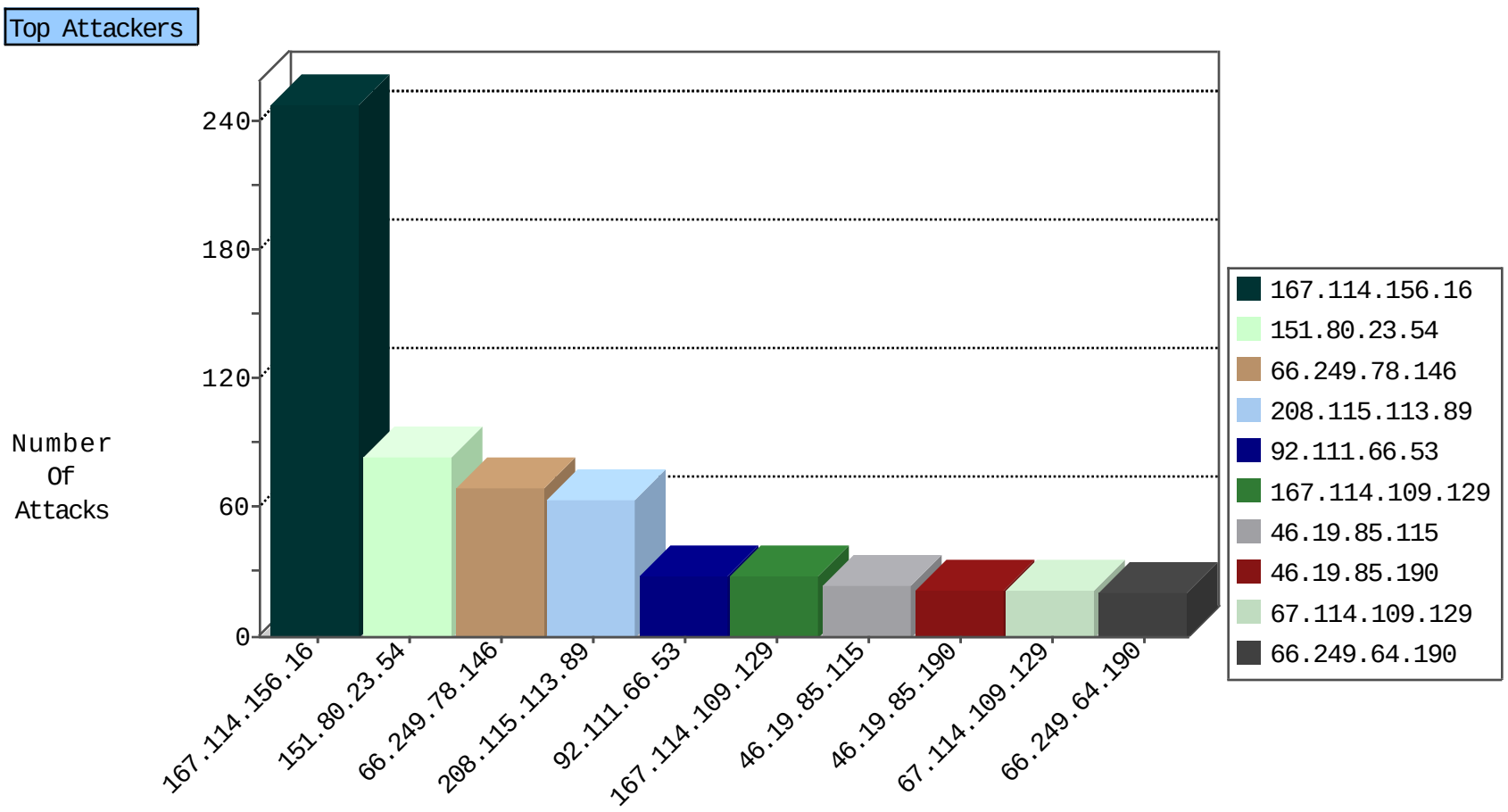
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-28-2016-01:04:12 to 04-28-2016-02:04:12

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	HTTP-POST-Segmented-DoS	dest-reset	9651
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2093
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
141.0.15.36	Norway	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	3
141.0.15.36	Norway	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
217.112.96.194	Italy	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
1.251.238.57	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
31.148.219.200	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.48	Lithuania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
80.101.214.86	Netherlands	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1

04-28-2016-01:04:12 to 04-28-2016-02:04:12

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-01:04:12 to 04-28-2016-02:04:12

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
66.249.88.65	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
107.158.255.194	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
91.193.74.175	147.237.77.226	Gibraltar	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.16.45.243	147.237.77.178	Bulgaria	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
87.70.32.236	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
213.16.45.243	147.237.77.178	Bulgaria	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
58.218.204.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.178.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
163.172.140.23	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.202.120.146	147.237.0.33	Japan	idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.193.74.175	147.237.77.179	Gibraltar	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
213.16.45.243	147.237.77.178	Bulgaria	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.178.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
161.202.120.146	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1

04-28-2016-01:04:12 to 04-28-2016-02:04:12

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	69
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
151.80.23.54	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
151.80.23.54	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
92.111.66.53	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.70.32.236	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.85.115	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.108.195.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
67.114.109.129	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
67.114.109.129	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.249.32.69	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.13.18.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.88.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
167.114.109.129	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	8
167.114.109.129	Canada	147.237.72.156	aman.idf.il	SYN Attack		reject	7
167.114.109.129	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.222.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.18.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.250	Israel	147.237.77.243	mobile.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
141.0.14.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.109.129	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.142.239.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.12.81	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.217.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.216.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.210.184.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.31.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.70.51.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.70.86.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-28-2016-01:04:12 to 04-28-2016-02:04:12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	6
46.19.85.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	4
176.13.18.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.195.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.177.169.247	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 79.177.169.247	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
109.64.99.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.71.88.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.186.18.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.213.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 46.119.127.129	Block	2
106.186.113.132	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
2.53.139.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.182	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
108.26.200.145	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
5.28.130.226	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.70.32.236	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
46.19.85.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.169.247	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
5.29.126.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.119.127.129	Ukraine	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
46.121.193.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
90.162.241.7	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 90.162.241.7	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
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14322-he/dover.aspx„′ƒ¬¯„,¬¿„,¬½„′×′₪′ƒ¬¯„,¬¿„,¬½	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
65.55.210.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.148.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.7	Italy	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1

04-28-2016-01:04:12 to 04-28-2016-02:04:12