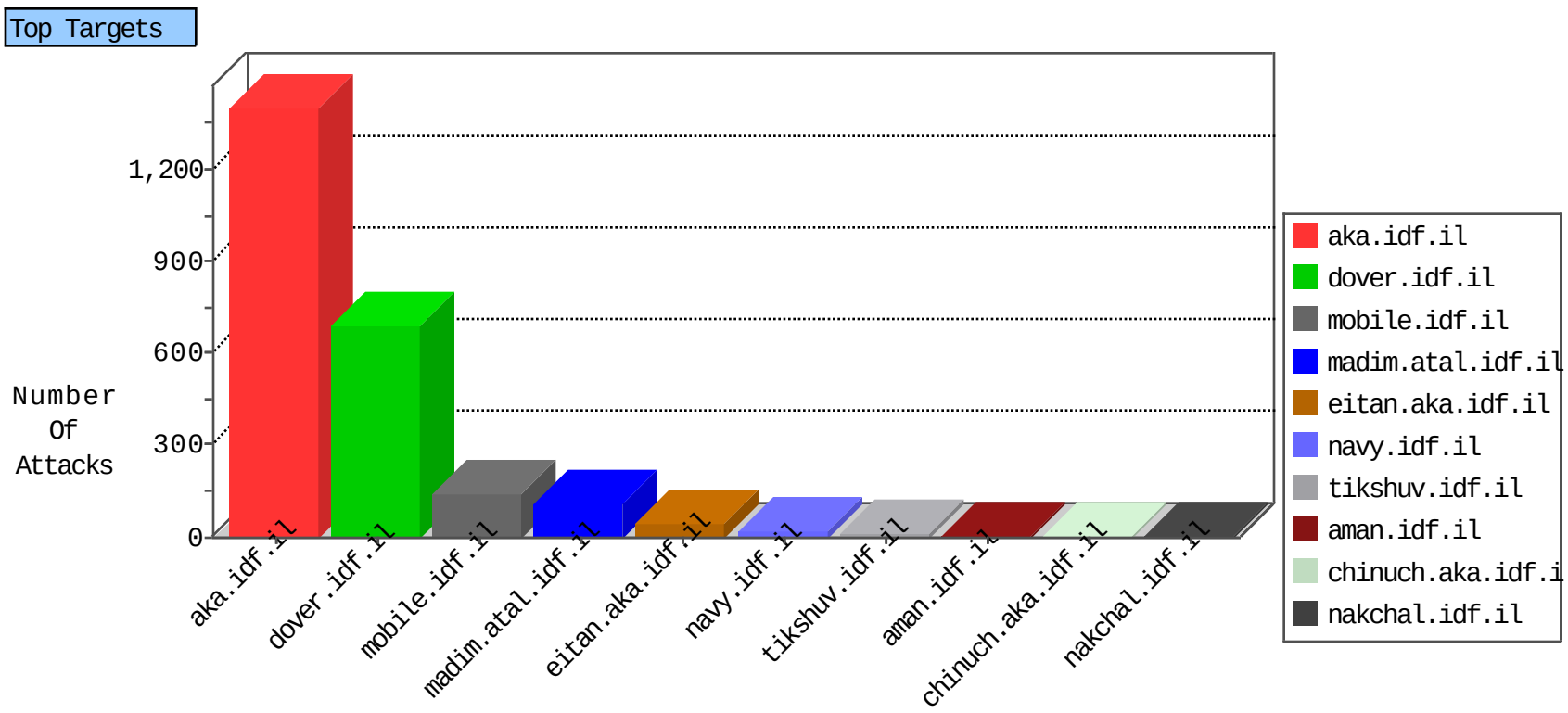
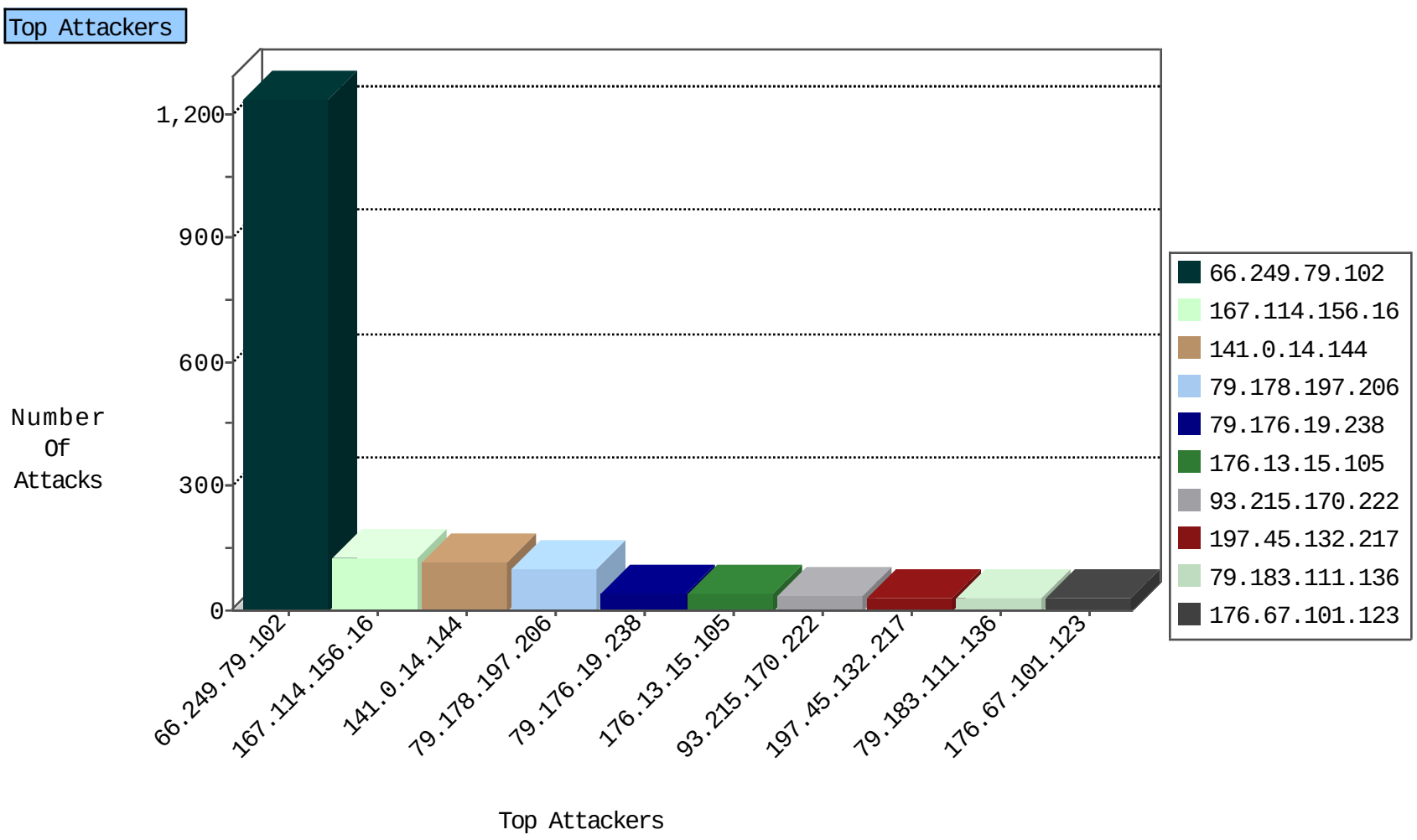
04-29-2016-22:04:07 to 04-29-2016-23:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-29-2016-22:04:07 to 04-29-2016-23:04:07

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	5331
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	358
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.174.54.63	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-29-2016-22:04:07 to 04-29-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.138.174.219	Japan	147.237.77.19	law-forum.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-29-2016-22:04:07 to 04-29-2016-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.102	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1190
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.31.86.178	147.237.76.200	France	eitan.aka.idf.il	Tehila - Perl LWP with fake user agent	2
183.3.202.115	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
112.169.100.157	147.237.76.176	Korea, Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
210.15.242.7	147.237.76.39	Australia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.34.99	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
208.67.1.225	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.193.74.175	147.237.76.202	Gibraltar	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.225	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
112.169.100.157	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
208.67.1.225	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.214.34.99	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.225	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.193.74.175	147.237.72.156	Gibraltar	aman.idf.il	ET SCAN NMAP -sS window 1024	1

04-29-2016-22:04:07 to 04-29-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.144	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
93.215.170.222	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.176.19.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
176.13.15.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.67.101.123	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
84.111.13.77	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
79.183.111.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.116.169.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
188.209.52.109	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
77.127.133.202	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.161.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
73.247.67.23	United States	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
37.142.72.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.96.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.180.200.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	9
79.180.200.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.179.96.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
97.74.24.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.110.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.195.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.22.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-29-2016-22:04:07 to 04-29-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.197.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
79.176.19.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
176.228.159.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.116.169.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.183.111.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
162.200.9.120	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	3
109.226.17.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.140.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.22.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	2
176.31.86.178	France	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
79.181.37.152	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
95.211.148.154	Netherlands	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
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
176.31.86.178	France	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 176.31.86.178	Block	1
82.166.61.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.66.182	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.8.204.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.125	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
54.196.104.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.8.214	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.31.86.178	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/categories.php	Block	1
87.70.67.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1

04-29-2016-22:04:07 to 04-29-2016-23:04:07