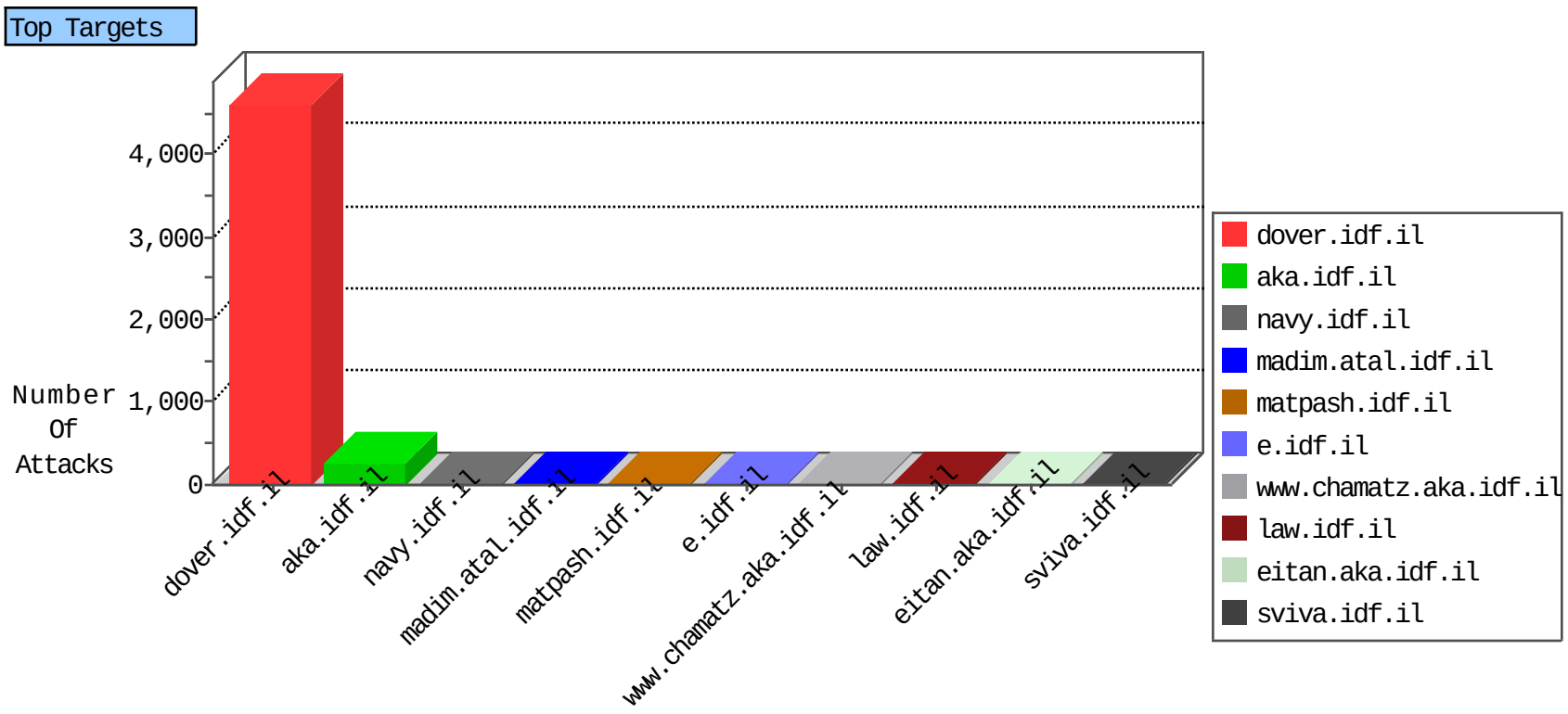
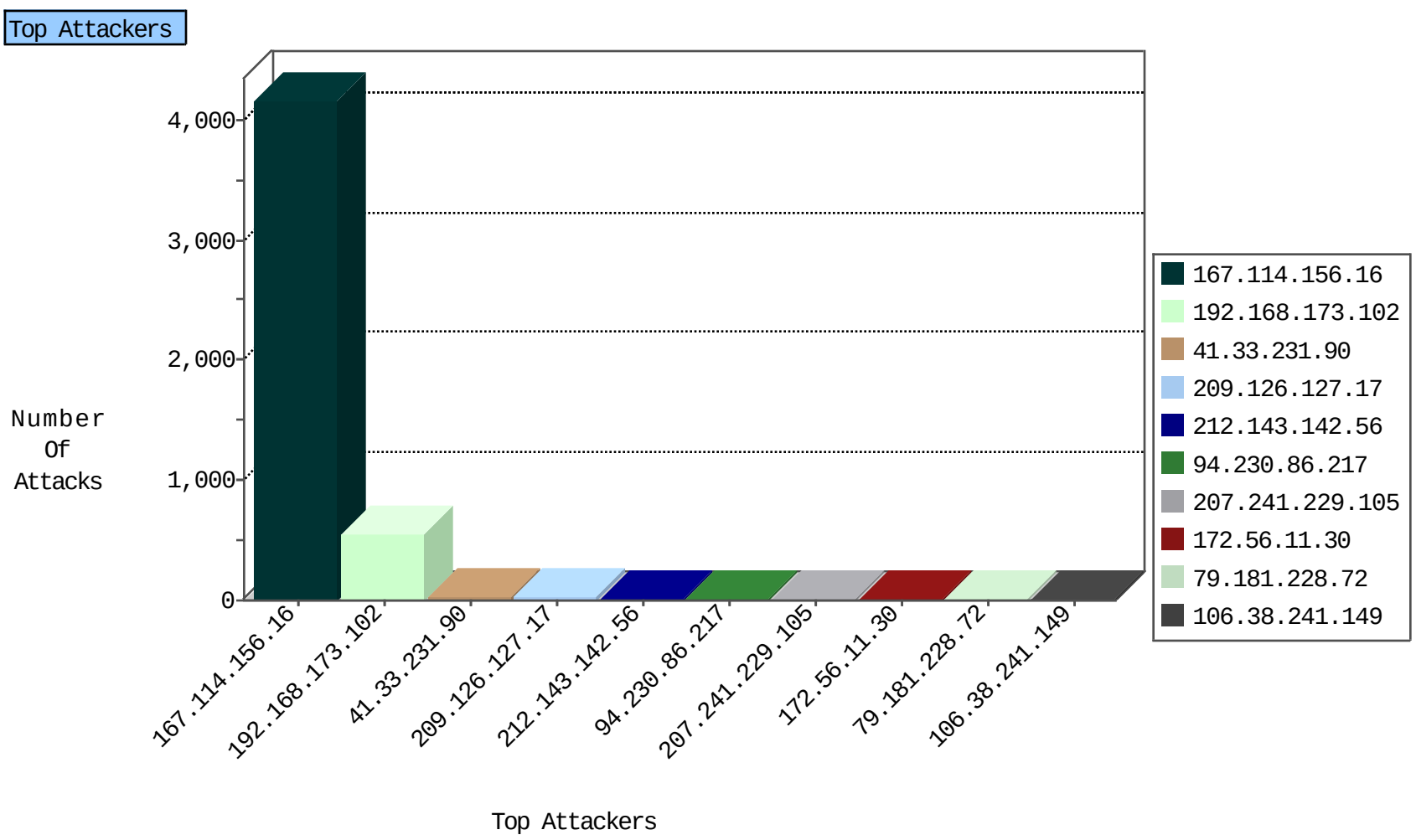
04-10-2016-05:04:08 to 04-10-2016-06:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-05:04:08 to 04-10-2016-06:04:08

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	Block_Ip_Web_In	drop	4158
209.126.127.17	United States	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	4
209.126.127.17	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.96	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
93.215.29.93	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
198.20.69.74	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
93.215.29.93	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.96	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
93.215.29.93	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
93.215.29.93	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.96	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
93.215.29.93	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.146.185	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1

04-10-2016-05:04:08 to 04-10-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.56.110.176	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
149.56.110.176	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.172	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-05:04:08 to 04-10-2016-06:04:08

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
121.183.38.187	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.72.217	Kazakstan	e.idf.il	ET SCAN NMAP -sS window 2048	1
24.182.16.6	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
24.182.16.6	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.37.99	147.237.72.217	Mexico	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.173.37.99	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.72.217	Kazakstan	e.idf.il	ET SCAN NMAP -sS window 4096	1
88.204.187.90	147.237.72.217	Kazakstan	e.idf.il	ET SCAN NMAP -f -sS	1
24.182.16.6	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
201.173.37.99	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.74	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1

04-10-2016-05:04:08 to 04-10-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	342
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	207
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.241.229.105	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
172.56.11.30	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.228.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
94.230.86.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.34.11.42	Jordan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.229.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
184.105.139.124	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.50.87.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.26	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.236	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
134.35.140.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
96.89.29.253	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.199	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.47	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
1.152.96.20	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.238	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
96.89.29.253	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.207	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
120.132.84.157	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
1.152.96.20	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.29.79	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.253	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
99.253.154.134	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.112	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
180.94.74.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
143.229.238.173	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
99.253.154.134	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
70.39.186.222	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.247.231	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
134.35.140.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

04-10-2016-05:04:08 to 04-10-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.83.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
54.153.33.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
23.106.244.134	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
8.18.120.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
184.168.200.23	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
31.13.112.121	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
23.80.148.11	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
200.98.255.231	Brazil	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
66.249.83.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
119.81.52.55	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
23.81.247.225	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
68.180.228.37	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
54.147.44.247	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
157.55.39.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1238-he/refuah.aspx	Block	1
23.106.161.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/general.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1

04-10-2016-05:04:08 to 04-10-2016-06:04:08