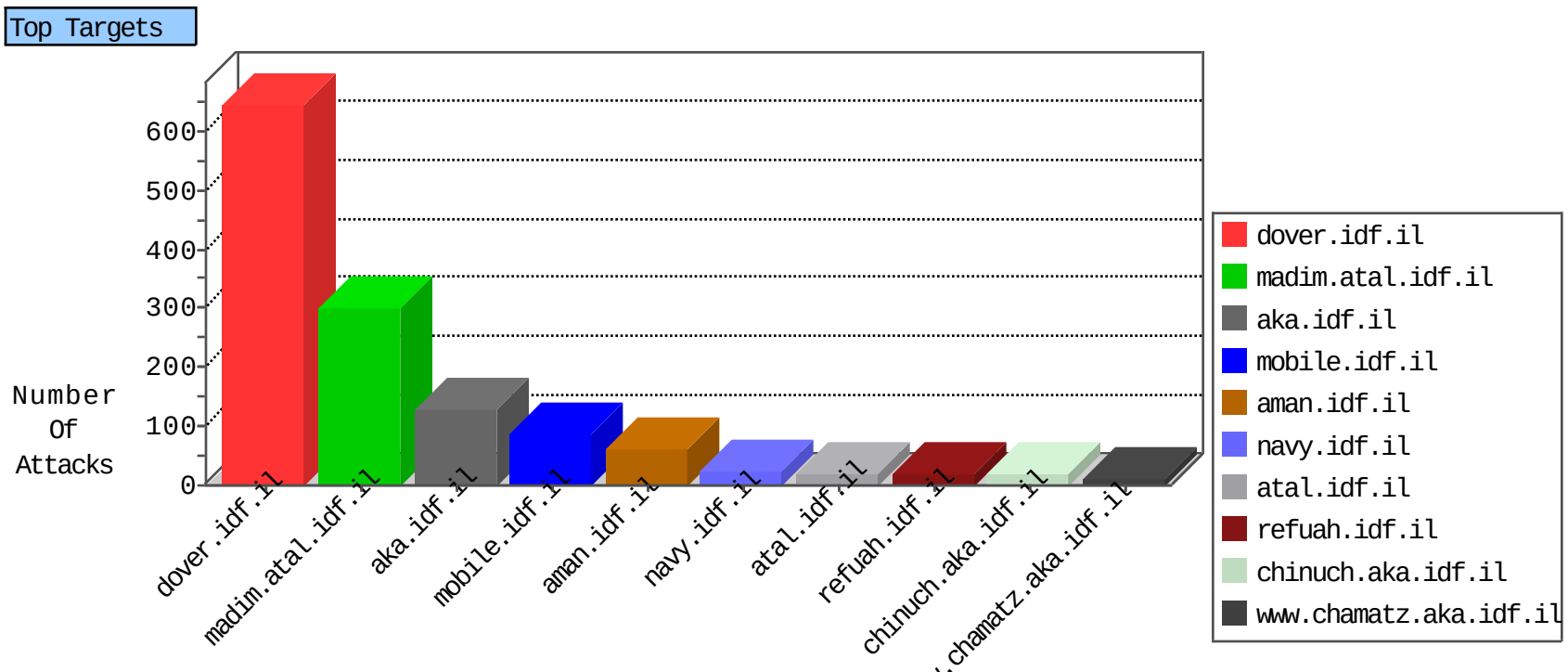
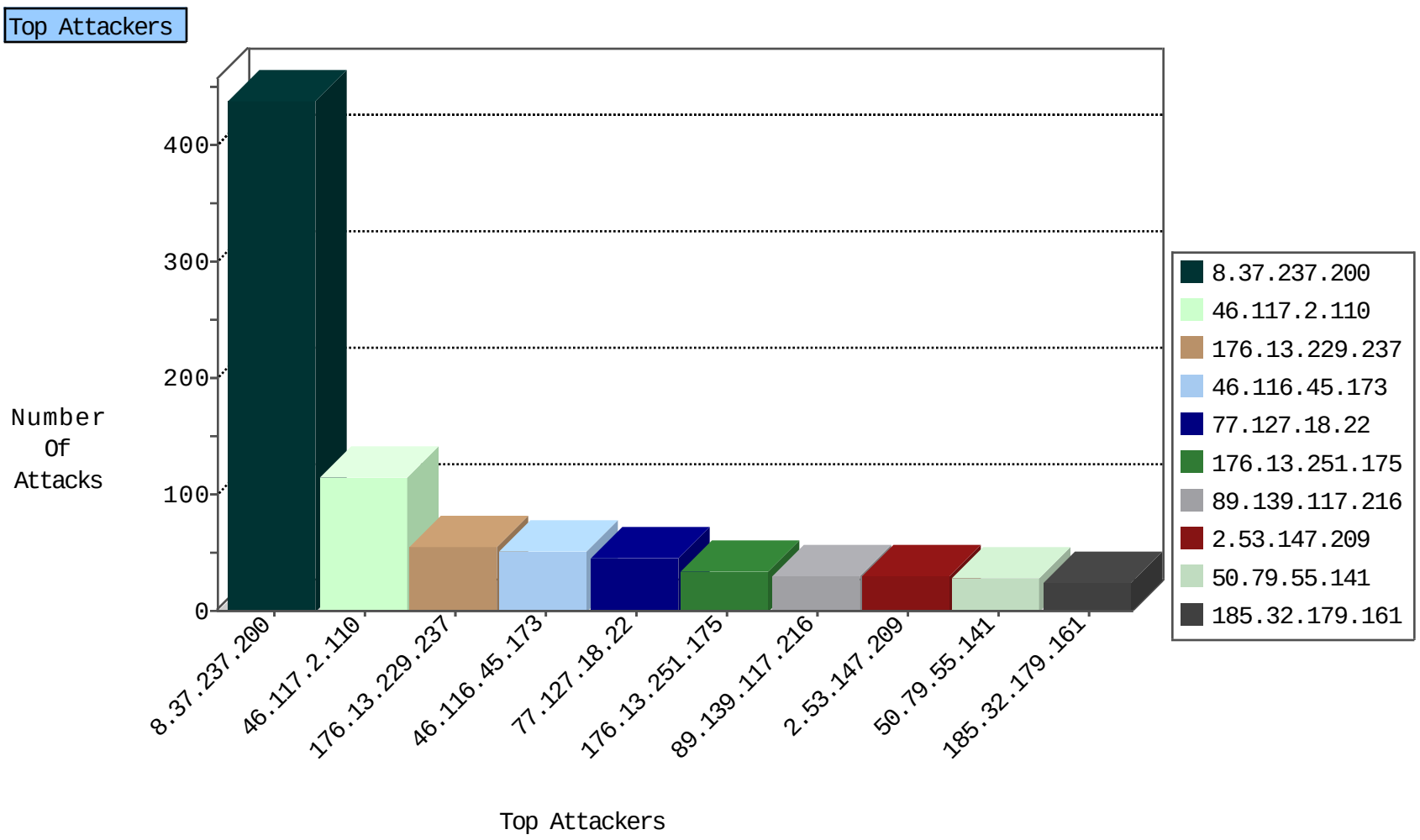
09-24-2016-19:04:00 to 09-24-2016-20:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-19:04:00 to 09-24-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.237.200	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
213.57.87.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.102.6.21	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
176.13.242.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.238.146.238	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
31.204.128.22	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
45.32.193.80	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
2.55.132.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

09-24-2016-19:04:00 to 09-24-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.103	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-24-2016-19:04:00 to 09-24-2016-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.66.212.249	147.237.77.216	Colombia	dover.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
80.68.56.82	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
69.129.141.35	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.93.158	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
8.37.237.200	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
190.66.212.249	147.237.77.216	Colombia	dover.idf.il	ET SCAN NMAP -sS window 2048	1
176.13.8.96	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
125.77.28.26	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
87.70.28.140	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
78.129.171.173	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	1
69.129.141.35	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
14.108.107.147	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.80.155.222	147.237.77.233	United States	atal.idf.il	Tehila - Perl LWP with fake user agent	1

09-24-2016-19:04:00 to 09-24-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.237.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	243
8.37.237.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	187
2.53.147.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
223.24.0.218	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
50.79.55.141	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
109.65.30.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.69.29.123	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
50.79.55.141	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
62.0.116.148	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
79.180.135.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.1.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.251.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
87.70.28.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.180.254.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.251.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.55.132.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.180.254.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.117.19.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.38.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.81.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.38.206	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.102.6.21	United States	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
84.94.69.115	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.117.2.110	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
213.57.70.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.243.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
93.173.119.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
98.221.243.125	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.242.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.242.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.121.145.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.251.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
98.221.243.125	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.251.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.6.19	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.38.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
87.70.36.47	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3

09-24-2016-19:04:00 to 09-24-2016-20:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.2.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.229.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.116.45.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
77.127.18.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
89.139.117.216	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	30
185.32.179.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.3.147.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
185.3.147.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
185.32.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.135.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
176.13.244.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.196.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.18	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
5.29.22.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
79.182.127.189	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.93.72	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2617.jpg	Block	1
87.71.32.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
77.138.153.54	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2349.jpg	Block	1
157.55.39.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.154.81.48	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.94.69.115	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.94.69.115	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
79.178.139.31	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.14	Block	1
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.69.115	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	1
77.138.90.17	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
109.65.161.245	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.38.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
37.26.149.206	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
84.108.94.178	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.97.87	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.29.220.238	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
109.65.185.123	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/maind9ea.html	Block	1
2.55.1.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
85.64.173.57	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.138.131.138	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
212.29.220.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1

09-24-2016-19:04:00 to 09-24-2016-20:04:00