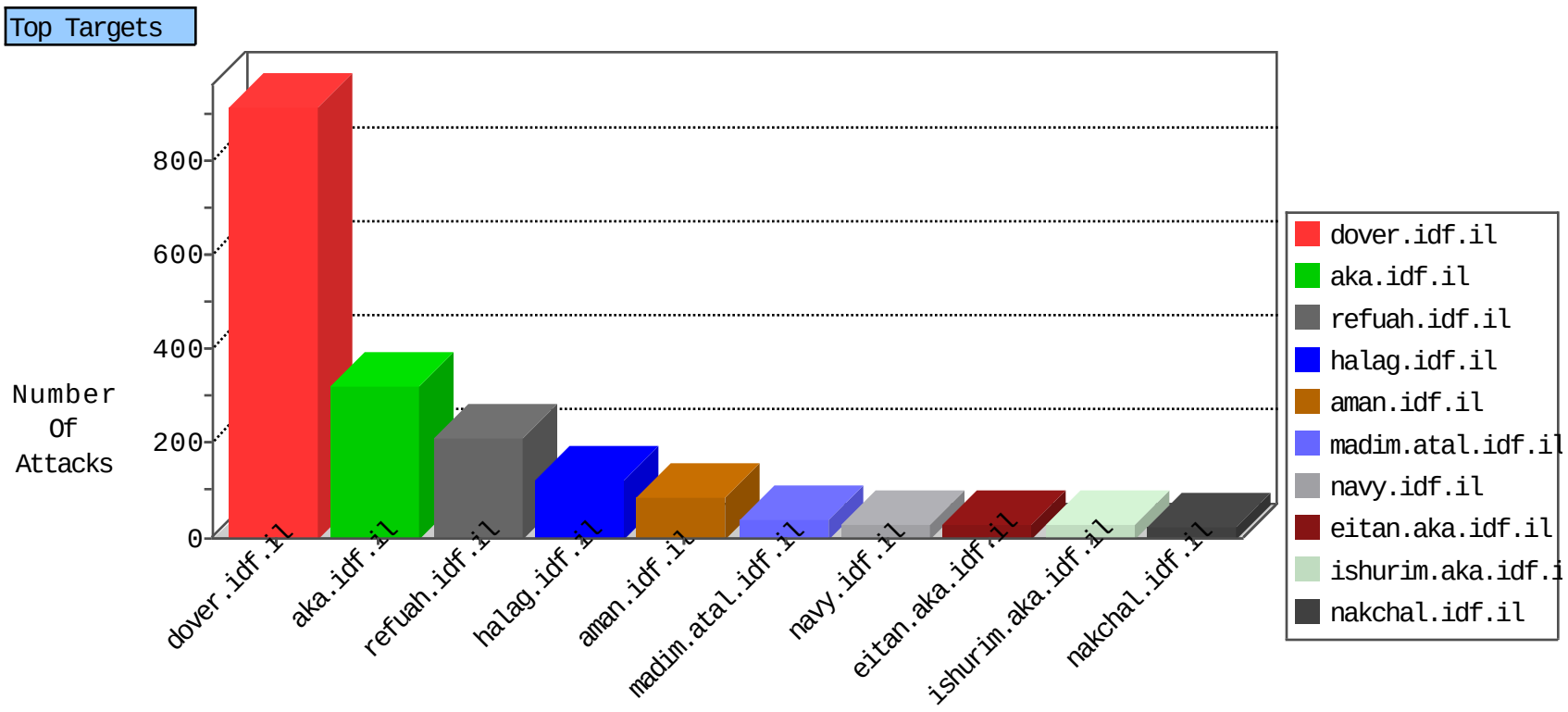
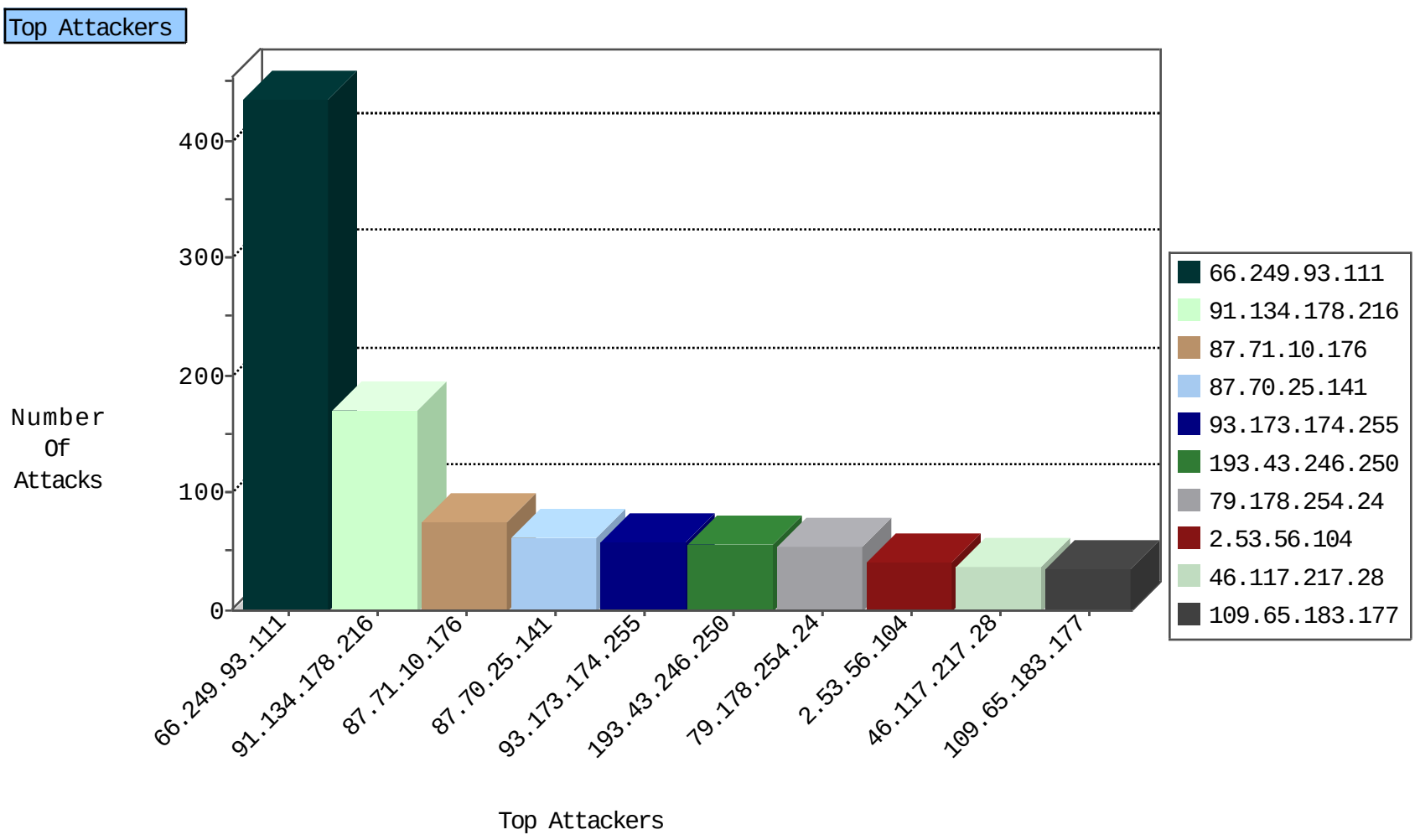
09-04-2016-18:04:01 to 09-04-2016-19:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-04-2016-18:04:01 to 09-04-2016-19:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	28
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
176.13.8.209	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
157.55.39.36	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.139.23.153	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
66.249.93.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
66.249.93.111	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.40.10.50	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.184.121	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
68.180.230.47	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.133.108	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
217.23.9.123	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
141.212.122.107	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
80.82.65.168	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
109.236.84.10	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
2.55.32.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.253.144.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
132.64.207.41	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.177.135.251	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

09-04-2016-18:04:01 to 09-04-2016-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-18:04:01 to 09-04-2016-19:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
208.100.26.228	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
179.32.103.202	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.40.71.107	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.64.226	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
65.23.114.140	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
211.141.78.56	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.77.91.109	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.56.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
65.23.114.140	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
219.127.49.142	147.237.76.31	Japan	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
65.23.114.140	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
211.141.78.56	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

09-04-2016-18:04:01 to 09-04-2016-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop		drop	211
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	140
87.71.10.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
87.70.25.141	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
2.53.56.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
109.65.183.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
46.117.217.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	32
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
46.19.86.201	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	26
80.179.9.115	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	24
80.179.9.7	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	23
79.178.254.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
107.167.107.124	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
79.178.254.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
91.134.178.216	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
91.134.178.216	Bulgaria	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
91.134.178.216	Bulgaria	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
79.178.254.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
91.134.178.216	Bulgaria	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
91.134.178.216	Bulgaria	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
91.134.178.216	Bulgaria	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
77.138.106.113	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
91.134.178.216	Bulgaria	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
91.134.178.216	Bulgaria	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.86.3	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	13
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
2.53.4.254	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
82.81.128.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
213.57.185.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.102.169.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
80.246.133.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.191	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.129.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.117.217.28	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
37.26.147.223	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.236.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.224.117	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6

09-04-2016-18:04:01 to 09-04-2016-19:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.21.160	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	29
2.53.13.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	11
2.55.166.59	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.55.166.59	Block	8
5.11.40.173	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
109.66.182.104	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.182.104	Block	3
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.47.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.101.179	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.68.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.6.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
217.132.4.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
108.63.124.13	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
82.81.101.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.51.10	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	2
79.180.212.14	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
160.39.33.240	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/glyus	Block	1
77.138.195.104	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.222.222	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.67.14	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
78.46.42.235	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
109.66.182.104	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
87.70.25.141	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.181.8.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
192.114.3.241	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
77.138.209.14	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
109.65.74.187	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.128.44	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.176.31.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
200.76.91.156	Mexico	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.139.98.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.55.166.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms.asp	Block	1
80.246.130.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.5.142	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mpm	Block	1
37.26.147.223	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.183.177	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
112.134.32.129	Sri Lanka	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
82.81.101.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.32.12	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/miluim/	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
37.26.148.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.4.57	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1

09-04-2016-18:04:01 to 09-04-2016-19:04:01