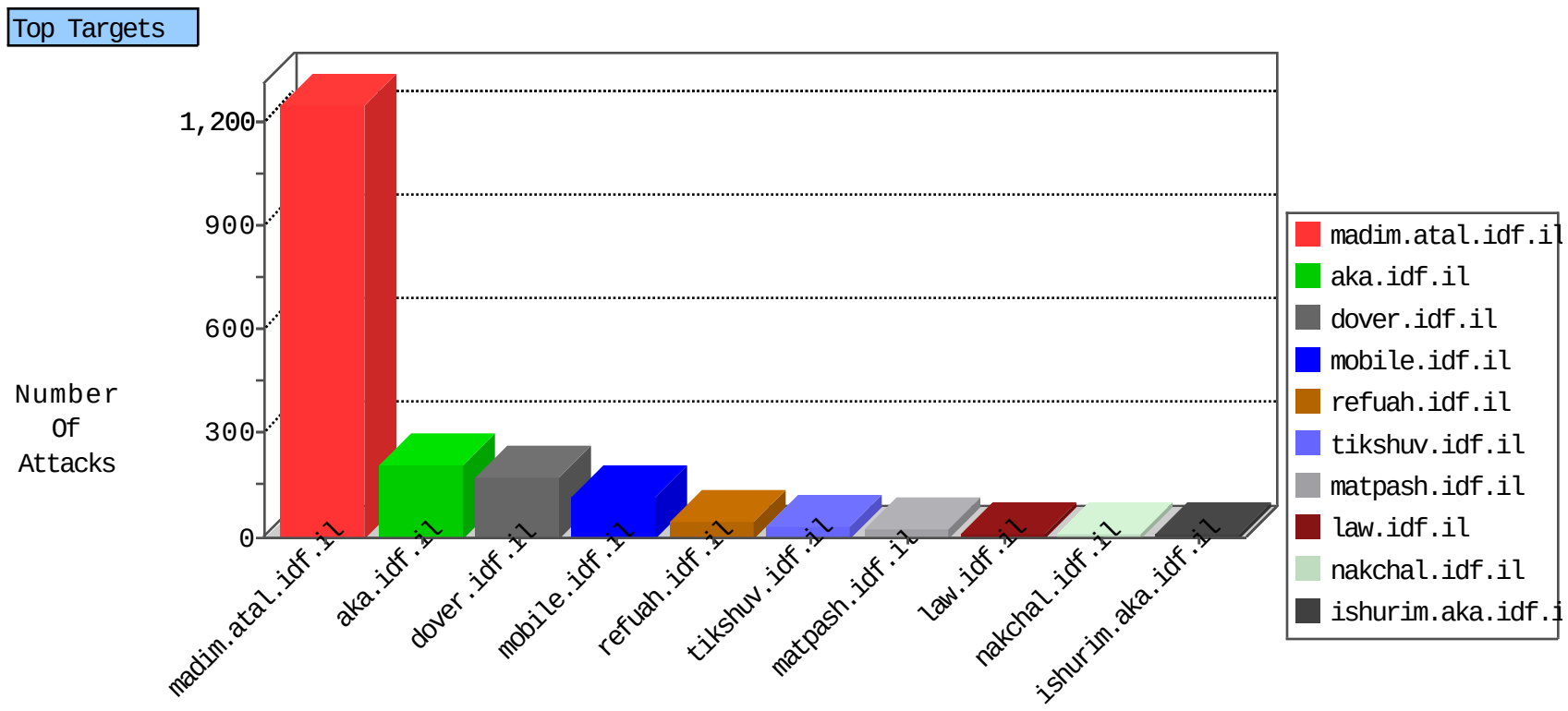
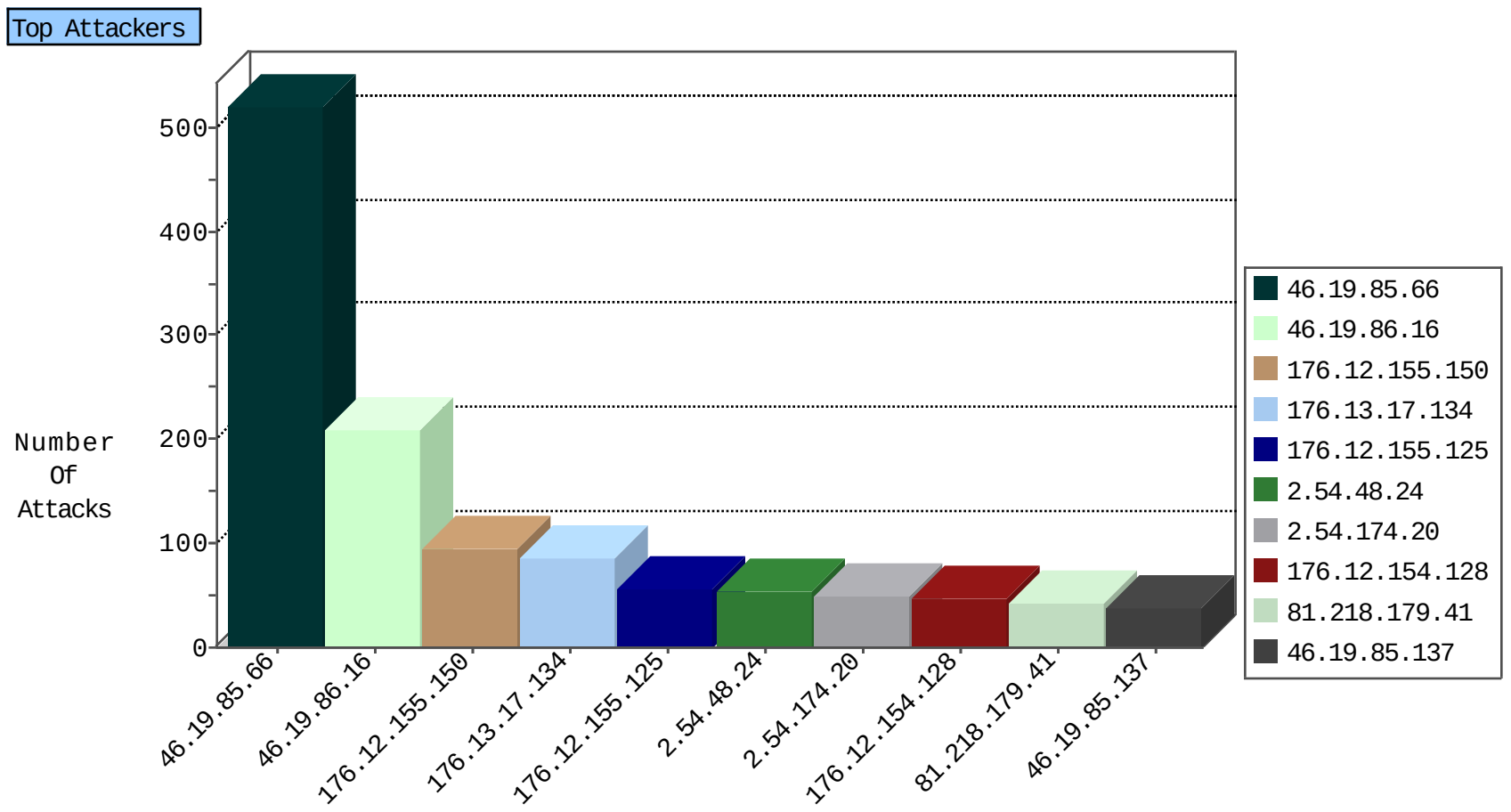
02-03-2016-09:04:05 to 02-03-2016-10:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-03-2016-09:04:05 to 02-03-2016-10:04:05

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	HTTP Page Flood Attack	drop	20
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
116.26.248.225	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
217.146.91.36	United Kingdom	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
116.26.248.225	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-09:04:05 to 02-03-2016-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.121.115.7	Malaysia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-03-2016-09:04:05 to 02-03-2016-10:04:05

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	3
94.159.196.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.167.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.179.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.147.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.10.152.67	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.50.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.61.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.255.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.168.133.63	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.51.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.138.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.24.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.22.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
165.225.72.65	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.27.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.201.63	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

02-03-2016-09:04:05 to 02-03-2016-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.48.24	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.114.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.110.35.167	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	9
2.54.48.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.110.35.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
84.110.35.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
109.253.133.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.42.198	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.181.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.203	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.207.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
2.54.1.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.188.72	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.125.162.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.179.114.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.80.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.12.155.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.30.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.175.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.27.105.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.35.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.61.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.28.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.54.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
81.218.176.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-09:04:05 to 02-03-2016-10:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.81.240.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.73.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.80.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
176.12.155.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-09:04:05 to 02-03-2016-10:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	302
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.66	Block	103
176.12.155.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
176.13.17.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.12.155.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
176.12.154.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.54.174.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.18.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.48.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 216.72.40.185	Block	26
37.26.148.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
188.53.159.138	Saudi Arabia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	3
185.32.179.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.110.35.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
2.54.48.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
188.53.159.138	Saudi Arabia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.219.162.91	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
37.26.146.226	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.64.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.52.63.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.211	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
176.12.155.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 82.102.169.113 (Open Mode)	None	1
37.26.149.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in www.aka.idf.il/giyus/forum/	None	1
66.249.69.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/894-he	Block	1
46.117.222.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.88.123.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
37.26.146.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.64.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.52.156.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.28.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/drushâ€‹imâ€?	Block	1
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
45.72.67.253		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
5.29.230.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sackhar	Block	1

02-03-2016-09:04:05 to 02-03-2016-10:04:05