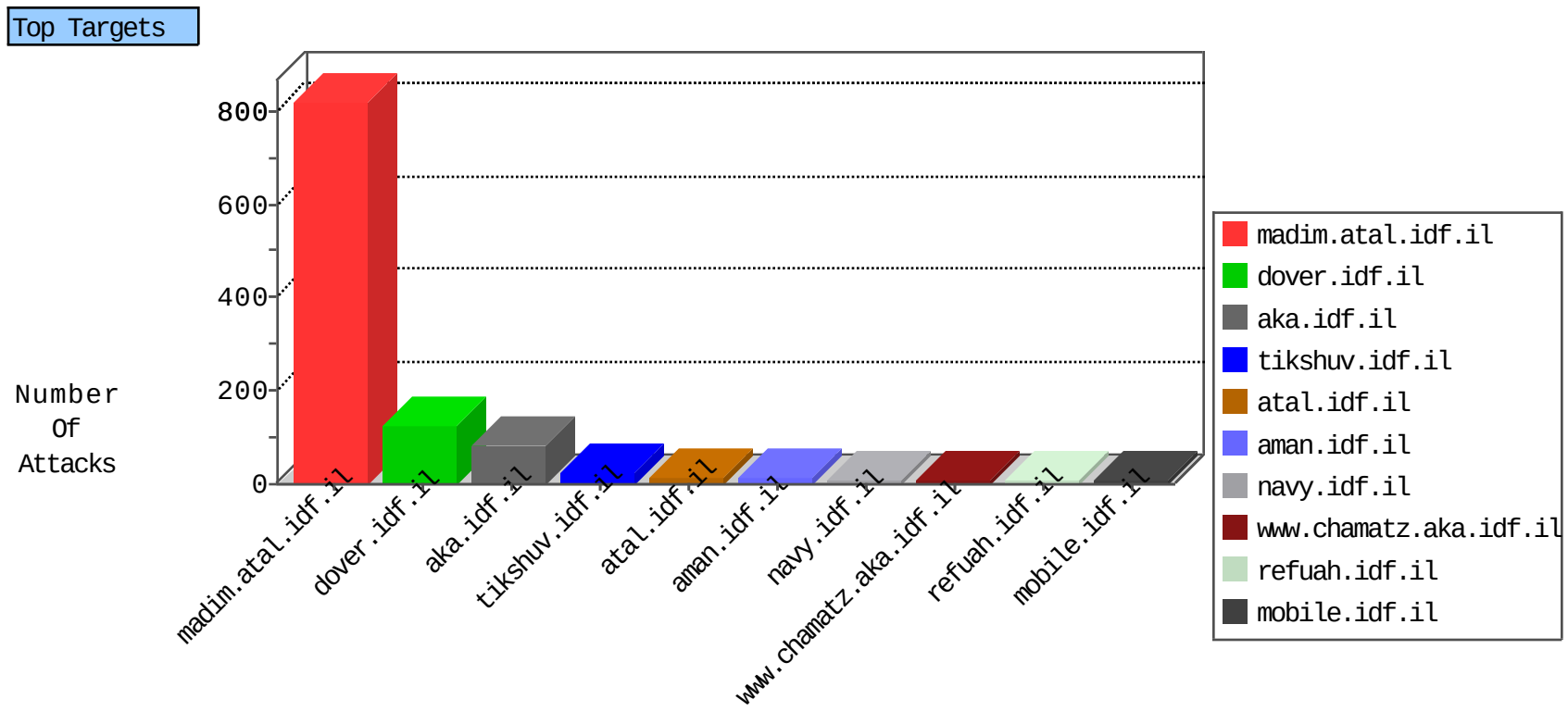
09-04-2016-10:04:08 to 09-04-2016-11:04:08

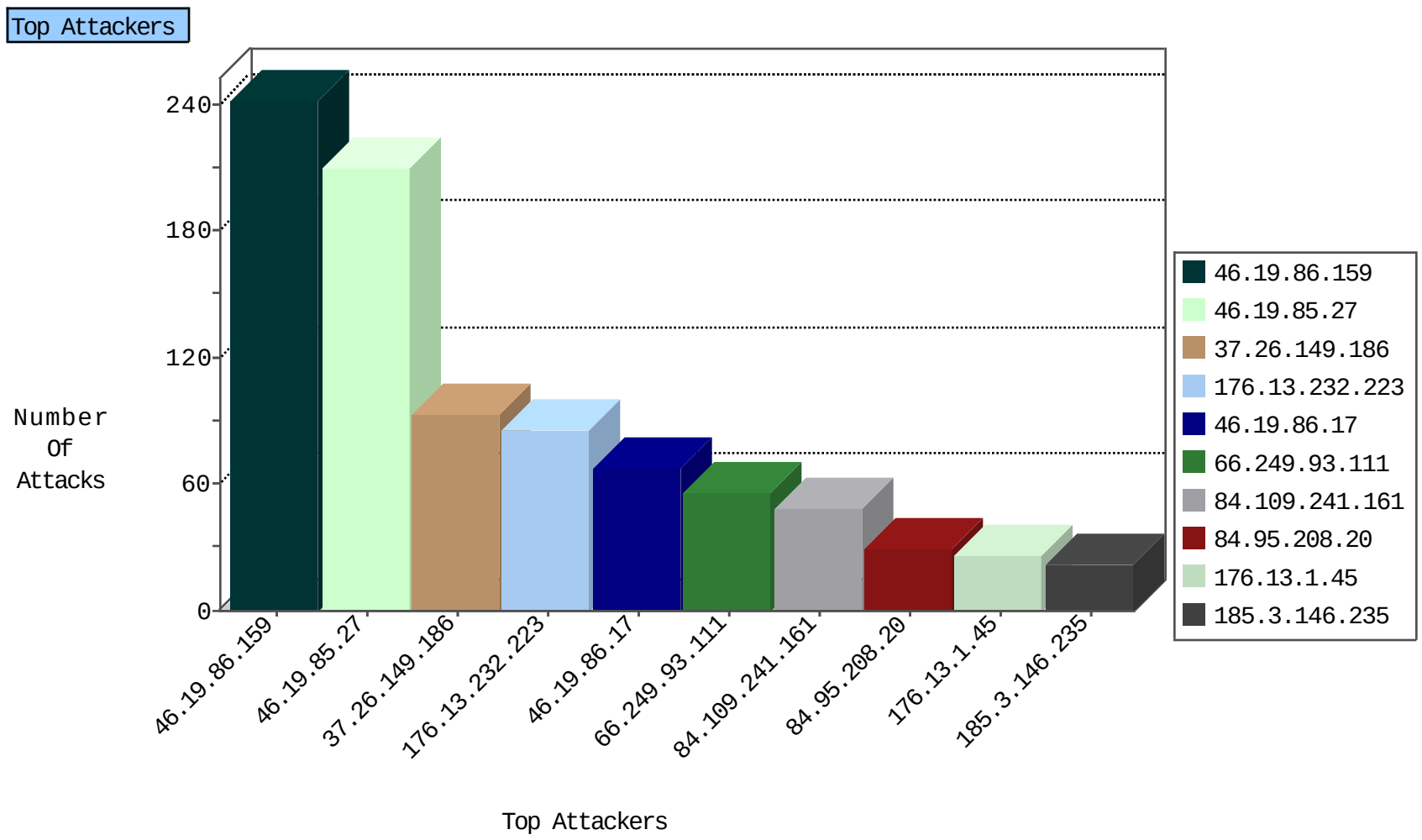
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-04-2016-10:04:08 to 09-04-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.183.36	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	2
62.219.193.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1
91.230.107.174	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
212.235.98.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-04-2016-10:04:08 to 09-04-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
163.172.29.9	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-04-2016-10:04:08 to 09-04-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.175.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.224.109.175	147.237.77.176	Germany	matpash.idf.il	ET SCAN Potential SSH Scan	1
85.250.137.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.74.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
139.162.13.205	147.237.76.86	Singapore	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
79.179.8.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.127.0.45	147.237.76.198	Italy	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.53	147.237.72.167	Israel	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
115.64.47.199	147.237.72.166	Australia	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.4.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.28.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.244.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
2.53.170.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.168.20.83	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.57.62.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.246.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.77.91.109	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.130.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.232.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.149.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.162.13.205	147.237.8.45	Singapore	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.90.88.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.127.0.45	147.237.76.198	Italy	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
46.19.85.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.139.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.91.75.231	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
2.55.50.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1

09-04-2016-10:04:08 to 09-04-2016-11:04:08

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	SAM rule	drop	51
185.3.146.235	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.86.3	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
46.117.217.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
46.19.86.243	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	8
109.253.205.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.239	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
176.13.230.91	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.255	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	4
46.19.86.243	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
185.89.217.226	Netherlands	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
46.19.85.185	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.201	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	3
46.19.85.0	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.56	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
84.110.179.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
112.215.151.191	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.178	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
185.3.146.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.18.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
216.218.206.104	United States	147.237.0.35	akaws.idf.il	drop		drop	1
100.92.65.34		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.11.247	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.130.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.80.41.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.89.217.226	Netherlands	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
109.253.193.223	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
62.219.77.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.82	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.228.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.80.64.30	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.123	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
66.249.69.2	Israel	147.237.0.33	idf.il	drop		drop	1

09-04-2016-10:04:08 to 09-04-2016-11:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	242
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	210
37.26.149.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
176.13.232.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
84.109.241.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.13.1.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
93.172.200.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.109.241.161	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	8
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
80.246.137.77	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.137.77	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
87.69.195.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.73.241	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.158.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	2
80.246.133.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.26.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.109.241.161	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
80.246.137.77	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
109.67.128.237	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/templates/catalog/catalog.aspx	Block	1
79.179.222.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/cgi-bin/shitur/bookpage100598/iturfindpageexact.pl	Block	1
84.108.77.234	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
157.55.39.68	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/usercontrols/headerupper/	Block	1
87.69.195.235	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/giyus/qanda/default.asp	None	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
194.90.25.122	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/918-he/atal.aspx	Block	1
77.139.190.189	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus	Block	1
132.72.138.1	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

09-04-2016-10:04:08 to 09-04-2016-11:04:08