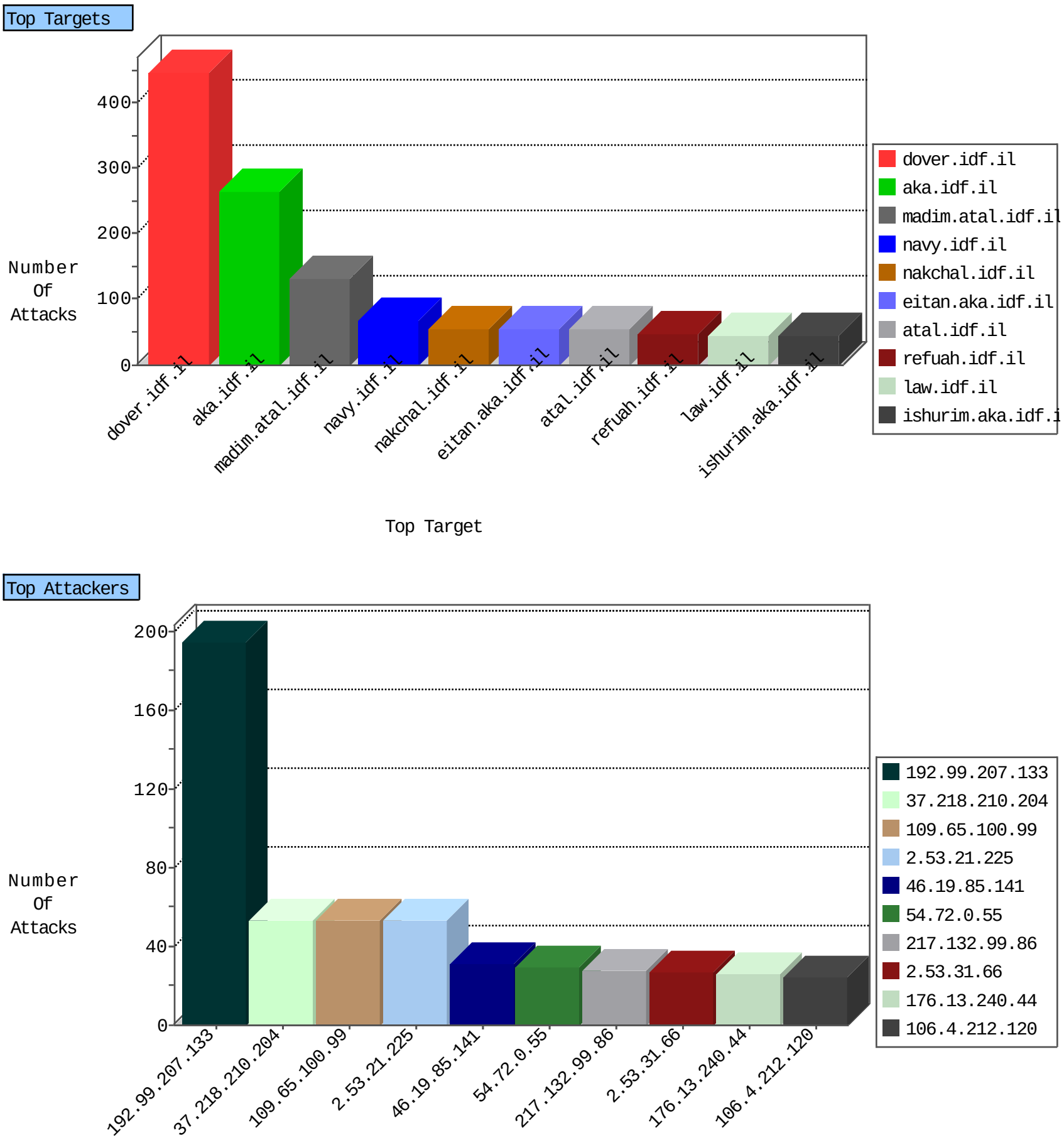
09-06-2016-17:04:02 to 09-06-2016-18:04:02

IDF Under Attack
Daily Report



09-06-2016-17:04:02 to 09-06-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.150.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-06-2016-17:04:02 to 09-06-2016-18:04:02

Top Attackers In IPS

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

09-06-2016-17:04:02 to 09-06-2016-18:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
93.158.203.197	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
86.3.248.114	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.121.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.30.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.18.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
169.46.2.146	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.137.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.72.167	Singapore	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.72.167	Singapore	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
23.91.75.231	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.197	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.34.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.195	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.5.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.226.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.7.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.26.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.231.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.162.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
116.12.175.233	147.237.72.167	Singapore	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.199.211.80	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.28.169.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-06-2016-17:04:02 to 09-06-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.218.210.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.65.100.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.53.31.66	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
80.246.136.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
109.65.100.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.186.73.18	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.226.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
106.66.200.16	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.27	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.28.133.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.179.41.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.67.113.18	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.146.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.86.27	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
157.55.39.145	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.47.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.236.177	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.234	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.55.20.131	Lithuania	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.29.236.177	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.117.76.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.50	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.142.185	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.234	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
207.46.13.93	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.43.92.50	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4

09-06-2016-17:04:02 to 09-06-2016-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.21.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.240.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
106.4.212.120	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.4.212.120	Block	17
106.4.212.120	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
192.116.165.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
79.177.31.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
176.13.1.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.37.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.165.35	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.116.165.35	Block	3
37.26.146.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	2
176.13.226.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.108.166	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
89.138.179.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.220	Block	2
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
176.228.178.31	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
207.46.13.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/	Block	1
84.109.235.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.235.191	Block	1
77.126.69.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
106.4.212.120	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
207.232.37.179	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
85.250.203.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	1
77.126.69.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter do in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.69.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.19.121.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.100.99	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
213.57.160.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
176.13.226.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.69.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.69.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
109.66.80.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19352-he/idfgdover.aspx	Block	1
46.117.76.72	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
2.53.55.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.168.205	France	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	Multiple Unauthorized URL Access from 66.249.76.75	Block	1
192.116.165.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/4/	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

09-06-2016-17:04:02 to 09-06-2016-18:04:02