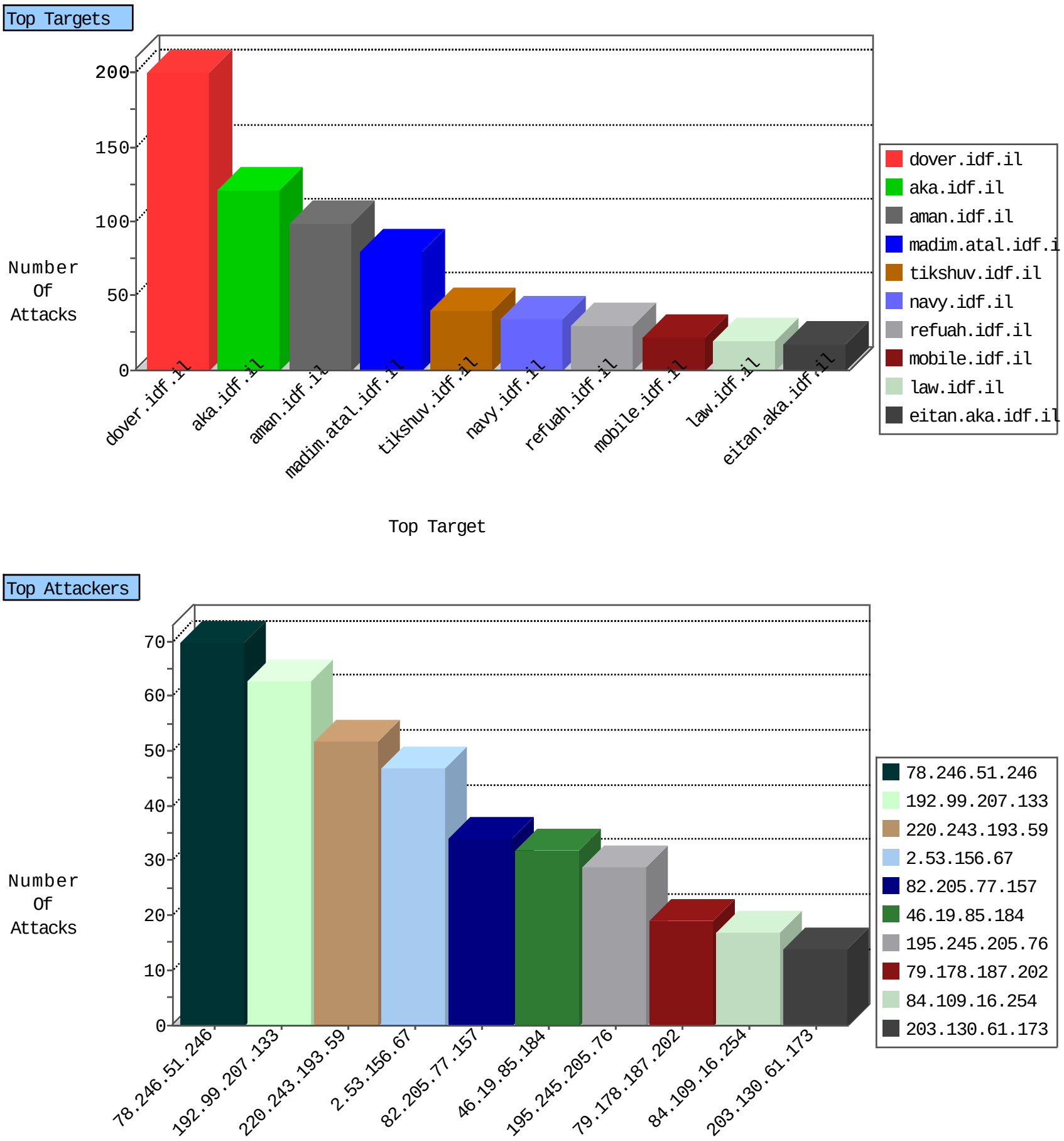
09-05-2016-17:04:02 to 09-05-2016-18:04:02

IDF Under Attack
Daily Report



09-05-2016-17:04:02 to 09-05-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.18.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
46.120.98.48	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
95.35.37.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
222.186.135.44	China	147.237.76.34	yohalan.idf.il	Black List	drop	1
109.236.84.10	Netherlands	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
209.126.136.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-05-2016-17:04:02 to 09-05-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-05-2016-17:04:02 to 09-05-2016-18:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.245.205.76	147.237.0.15	Russian Federation	kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
195.245.205.76	147.237.76.86	Russian Federation	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.8.46	Russian Federation	e.chinuch.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.8.24	Russian Federation	e.lifestyle.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.179	Russian Federation	e.mazi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.205	Russian Federation	prisha.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
85.250.118.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.201	Russian Federation	e.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
163.172.51.213	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.147.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.51.213	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -f -sS	1
222.186.58.176	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.136.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.39	Russian Federation	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
139.162.13.205	147.237.76.30	Singapore	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
213.151.46.39	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
79.178.88.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.77.233	Singapore	atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.73.143.36	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
74.81.77.141	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.77.234	Russian Federation	halag.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
109.67.25.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.138.89	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.77.212	Russian Federation	e.dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
104.197.206.193	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
45.32.138.89	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
97.105.173.114	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
186.170.81.82	147.237.77.233	Colombia	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.77.61	Russian Federation	e.cogat.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
2.53.9.50	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.il	ET SCAN Potential SSH Scan	1
85.250.116.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.197	Russian Federation	e.himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
163.172.51.213	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.42	Russian Federation	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
150.242.238.99	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.58.176	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.245.205.76	147.237.76.38	Russian Federation	e.e.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.179.99.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.77.233	Singapore	atal.idf.il	ET SCAN NMAP -sS window 4096	1
213.8.204.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.8.45	Russian Federation	e.eitan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.176.86.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.243	Russian Federation	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
109.67.48.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-05-2016-17:04:02 to 09-05-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
78.246.51.246	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
82.205.77.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.184	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
217.194.202.17	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.184	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.247.84.33	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
82.166.198.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.179.99.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
213.8.182.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
193.26.217.114	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.143.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.120.122.219	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
81.218.66.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.34.167.8	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.34.167.8	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
87.69.148.92	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
138.246.253.19	Germany	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.208.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.179.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
118.171.218.247	Taiwan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.27.106.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.180.203.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
185.3.147.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.236.238.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
80.246.137.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.147.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3

09-05-2016-17:04:02 to 09-05-2016-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.156.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
79.178.187.202	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	19
84.109.16.254	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	17
2.53.42.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	5
109.253.150.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.12.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
71.179.102.57	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
176.13.237.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.15.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
66.249.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1305-he/refuah.aspx	Block	1
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method cept-Language: in URL he-il,he	Block	1
213.8.182.149	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
2.53.141.186	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
77.138.173.101	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
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
5.29.232.90	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.230.47	Block	1
2.53.141.186	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 2.53.141.186	Block	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
77.138.208.147	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/kurs/default.asp	Block	1
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
40.77.167.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
71.179.102.57	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
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/	Block	1
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/home.asp	Block	1
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
87.69.55.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
50.247.84.33	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
2.53.190.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.81.65	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.166	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
46.19.85.145	Israel	147.237.76.31	nakchal.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
109.66.182.104	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.15.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.101.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.214.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/home.aspx	Block	1

09-05-2016-17:04:02 to 09-05-2016-18:04:02