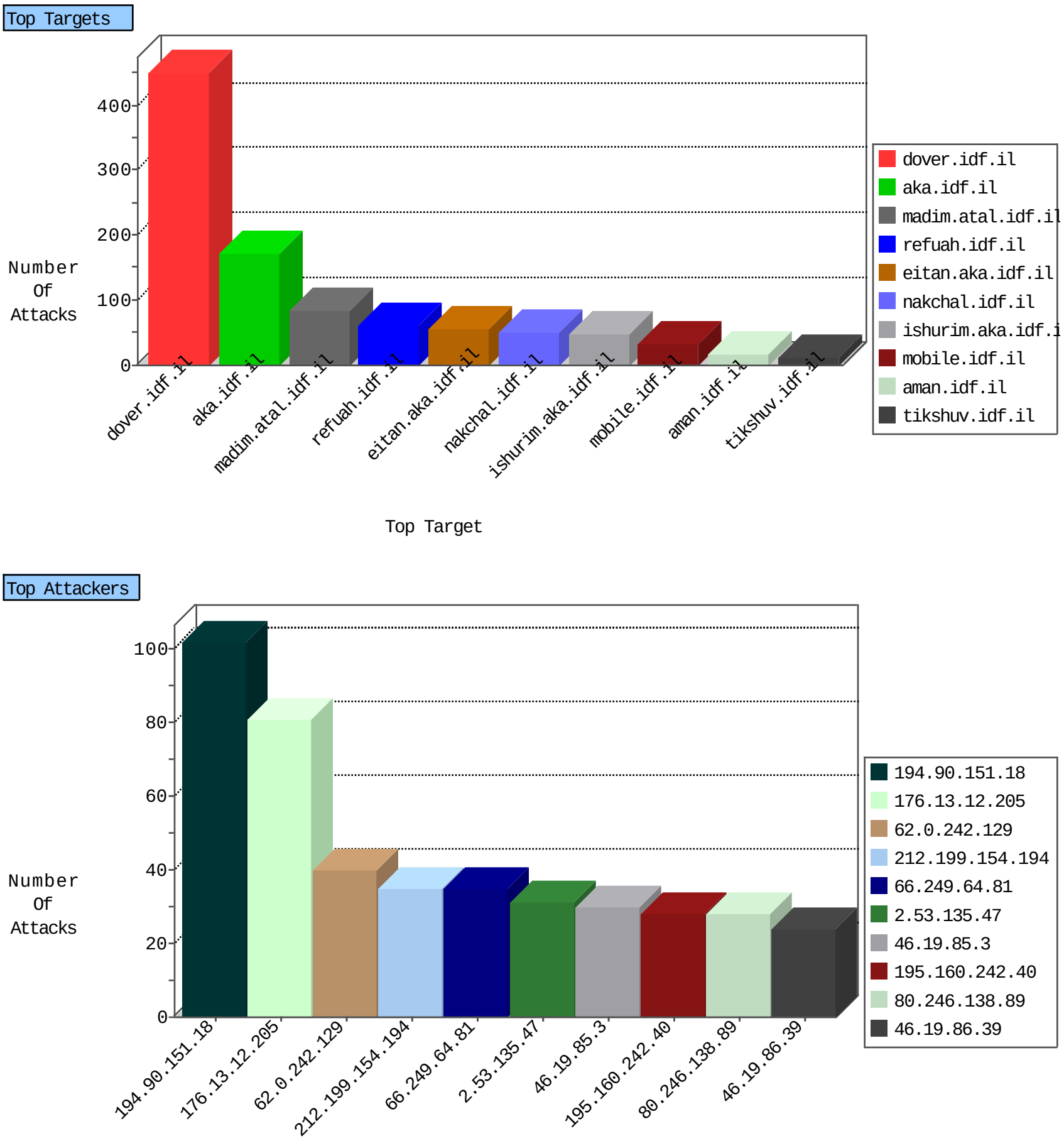
09-26-2016-08:04:09 to 09-26-2016-09:04:09

IDF Under Attack Daily Report



09-26-2016-08:04:09 to 09-26-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
176.13.12.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
77.139.101.27	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
209.126.136.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
46.19.86.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.1.105.91	Italy	147.237.76.201	e.atal.idf.il	Invalid L4 Header Length	drop	1
209.126.136.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
180.97.106.37	China	147.237.76.176	test.ncore.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-26-2016-08:04:09 to 09-26-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-26-2016-08:04:09 to 09-26-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.158	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -f -sS	1
193.169.70.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.103.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.108.29.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.42	Italy	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
79.183.63.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
139.162.187.89	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.84.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.170.36.68	147.237.76.42	India	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
114.112.83.142	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
42.159.197.39	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.60.121.232	147.237.76.86	Portugal	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
42.116.29.68	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 2048	1
42.116.29.68	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -f -sS	1
211.149.219.167	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
191.96.249.189	147.237.76.31	Chile	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.31.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.145.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.31.34.244	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
114.112.83.142	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.245.186.227	147.237.77.216	Indonesia	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.156.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.159.197.39	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 4096	1
42.116.29.68	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
218.87.109.253	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

09-26-2016-08:04:09 to 09-26-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.151.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
176.13.12.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.64.81	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.242.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	19
46.19.85.3	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
80.246.138.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
2.55.8.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.3	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
207.232.41.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.242.129	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.13.12.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
2.53.23.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.199.251.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
45.74.1.196	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	7
176.13.251.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.251.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.246.138.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.192.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.13.156	Israel	147.237.72.166	aka.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
46.19.86.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.201	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.118.36.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.85	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.195.103.241	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.251.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
80.246.138.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.189.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.12.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-26-2016-08:04:09 to 09-26-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.135.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.237.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.53.54.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
194.90.99.193	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	6
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
5.28.158.171	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
109.253.231.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
118.192.160.145	China	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 118.192.160.145	Block	3
2.53.57.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.99.193	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	3
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.249.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.146.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.131.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.227.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.27	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.138.54.90	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
46.19.86.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
66.102.8.142	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.76.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.64.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1149-en/eitan.aspx	None	1
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/undefined/	Block	1
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.64.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
66.102.9.8	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
180.76.15.26	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
66.249.64.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/999-en/eitan.aspx	None	1
96.126.109.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
66.249.64.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1084-en/eitan.aspx	None	1
109.253.244.53	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.53.147.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
206.246.150.226	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/index.php	Block	1
66.249.64.85	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
109.66.121.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58608&docid=78560	Block	1
66.249.75.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1085-en/eitan.aspx	None	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
80.178.220.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/recruitlane.aspx	Block	1
212.199.185.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.85	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1001-en/eitan.aspx	None	1
54.179.147.31	Singapore	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/web-console/serverinfo.jsp	Block	1
176.13.249.54	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.141.184	Israel	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	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.81	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1086-en/eitan.aspx	None	1

09-26-2016-08:04:09 to 09-26-2016-09:04:09