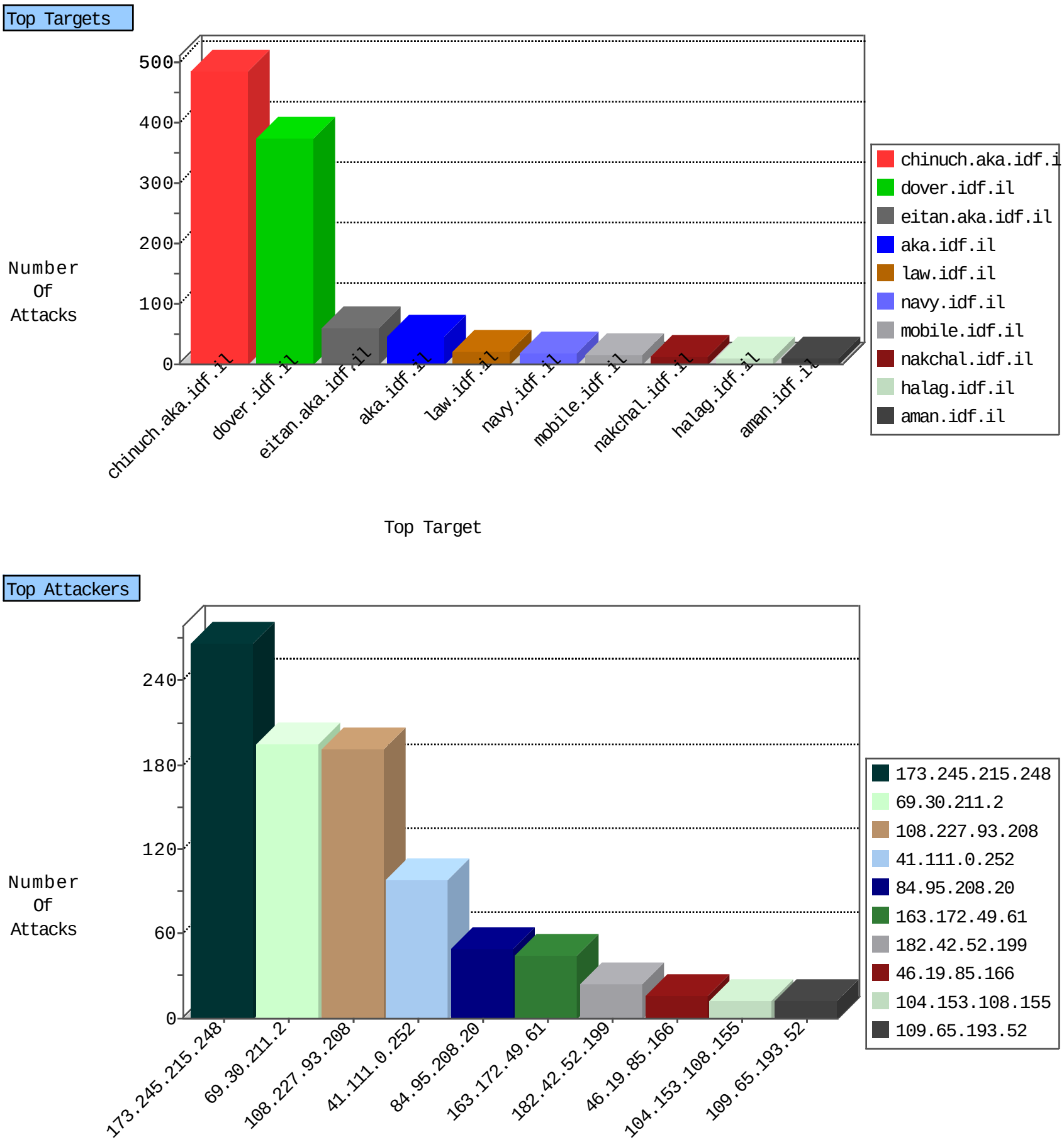
09-24-2016-10:04:07 to 09-24-2016-11:04:07

IDF Under Attack Daily Report



09-24-2016-10:04:07 to 09-24-2016-11:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.204.224.237	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
69.30.193.250	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
121.86.173.9	Japan	147.237.76.197	e.himush.idf.il	Black List	drop	2
69.30.226.219	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
204.12.220.85	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
69.30.227.221	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
63.141.231.194	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
104.238.146.105	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
63.141.231.194	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
63.141.231.196	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
204.12.220.84	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
45.32.193.80	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
142.54.174.86	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
63.141.231.197	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1

09-24-2016-10:04:07 to 09-24-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	184
163.172.49.61	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	26
163.172.49.61	United Kingdom	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	8
163.172.49.61	United Kingdom	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	7
69.30.211.2	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	7
163.172.49.61	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
163.172.49.61	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-24-2016-10:04:07 to 09-24-2016-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.106.139.19	147.237.76.198	Ireland	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
46.161.40.17	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.153.198.10	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.221	147.237.0.33	Switzerland	idf.il	ET SCAN Potential SSH Scan	1
116.108.166.171	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.106.139.19	147.237.76.198	Ireland	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
73.176.200.52	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
194.106.139.19	147.237.76.198	Ireland	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
40.121.139.43	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
185.153.198.10	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.72.166	Ukraine	aka.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.221	147.237.77.74	Switzerland	law.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.197.148	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
83.217.218.164	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-24-2016-10:04:07 to 09-24-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.245.215.248	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	257
108.227.93.208	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	192
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
73.13.205.65	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.166	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.166	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.65.193.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.4.201	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.178.163.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.184.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.65.193.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
1.186.41.84	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
79.177.131.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.139.251.236	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
1.186.41.84	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.139.108.37	France	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.176.51.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.102.195.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.181.243.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
128.232.110.28	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.142.251.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.139.108.37	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.20	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.90.255.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.29.125.19	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
69.30.211.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.37.147	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.212	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.53.8.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.139.108.37	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.226.217.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.150.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
104.153.108.155	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
184.105.139.84	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.19	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-24-2016-10:04:07 to 09-24-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	30
182.42.52.199	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 182.42.52.199	Block	17
182.42.52.199	China	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	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
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
79.182.106.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/	Block	1
66.249.65.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22810-ar/dover.aspx	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
85.64.16.23	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
41.111.0.252	Algeria	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
66.249.64.71	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/m/	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.176	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
182.42.52.199	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
46.19.85.212	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
77.139.236.27	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/m/	Block	1
2.53.131.48	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
157.55.39.1	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
182.42.52.199	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
46.19.85.212	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method .xml in URL	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.178.252.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
37.142.118.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
180.76.15.13	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1

09-24-2016-10:04:07 to 09-24-2016-11:04:07