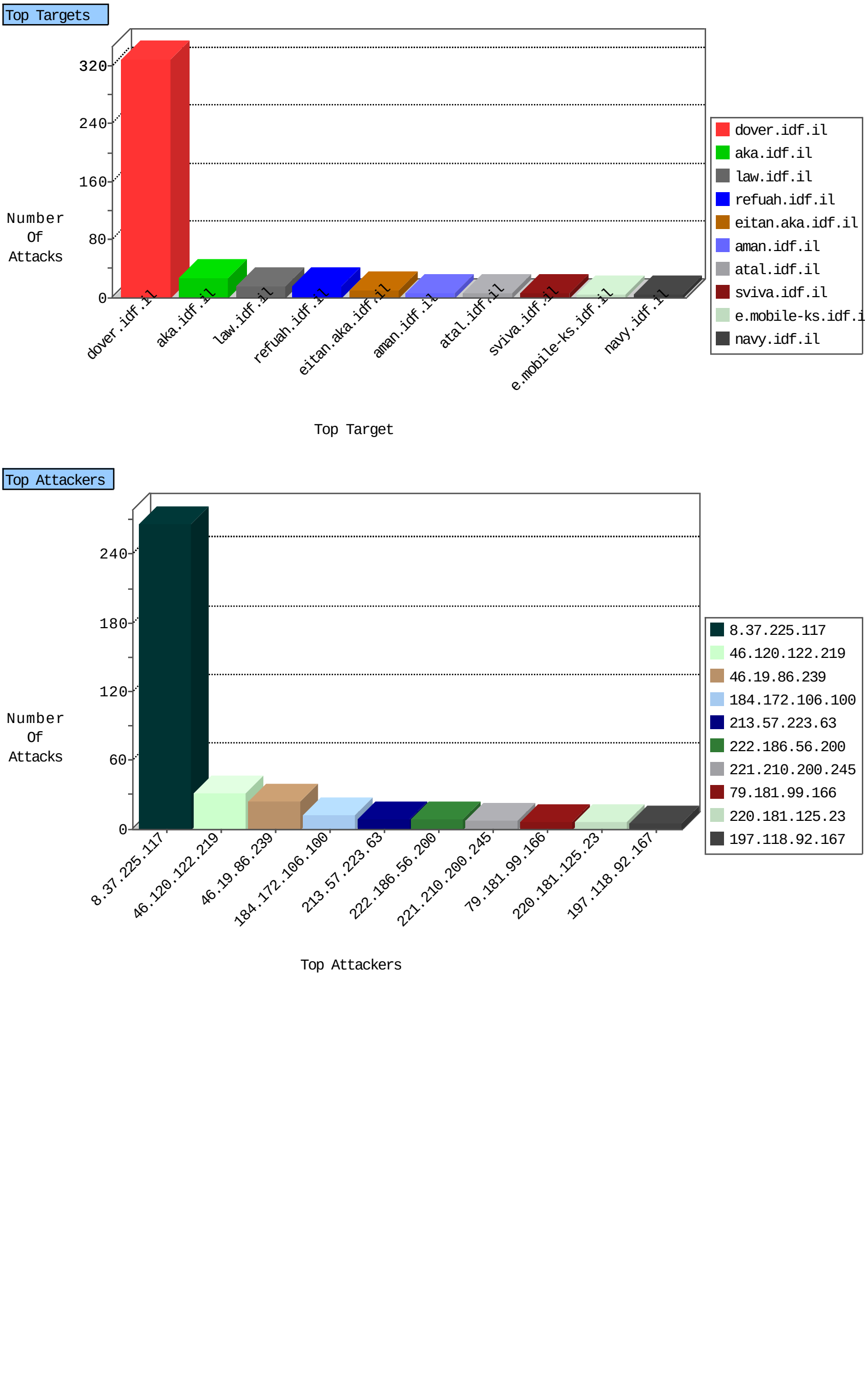
10-01-2016-04:04:08 to 10-01-2016-05:04:08

IDF Under Attack Daily Report



10-01-2016-04:04:08 to 10-01-2016-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.138.102.157	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
93.158.200.65	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
188.138.102.157	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
93.158.200.66	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
222.186.56.200	China	147.237.72.14	dover.idf.il(old)	JLM_Purple_Con_Limit_Tcp	drop	1
93.158.200.126	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1

10-01-2016-04:04:08 to 10-01-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.172.106.100	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
151.80.31.158	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

10-01-2016-04:04:08 to 10-01-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	11
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
218.209.68.240	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
222.186.56.200	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.114.60.162	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
222.186.56.200	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.46.166.235	147.237.77.176	China	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.56.200	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.194	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
221.210.200.245	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.114.60.162	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.56.200	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.200	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
115.202.212.70	147.237.77.212	China	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.56.200	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
221.210.200.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.255.90.133	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-01-2016-04:04:08 to 10-01-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	202
8.37.225.117	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	65
46.19.86.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
197.118.92.167	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
131.253.26.192	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
187.61.127.245	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.53.28.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.223.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.223.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.223.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
65.55.210.228	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
24.158.53.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.138.137	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.229.29.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.223.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.2	Israel	147.237.0.33	idf.il	drop		drop	1
141.212.122.20	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.160	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.130.189.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
213.57.223.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.112	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.18	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
216.218.206.122	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.21	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.237.106.206	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.21	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.115	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.117.240.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.22	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.16	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
93.174.93.218	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-01-2016-04:04:08 to 10-01-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	10
204.79.180.108	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
2.53.39.97	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.65.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22921-ar/dover.aspx	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1278-he/atal.aspx	Block	1
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.i	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.108	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1

10-01-2016-04:04:08 to 10-01-2016-05:04:08