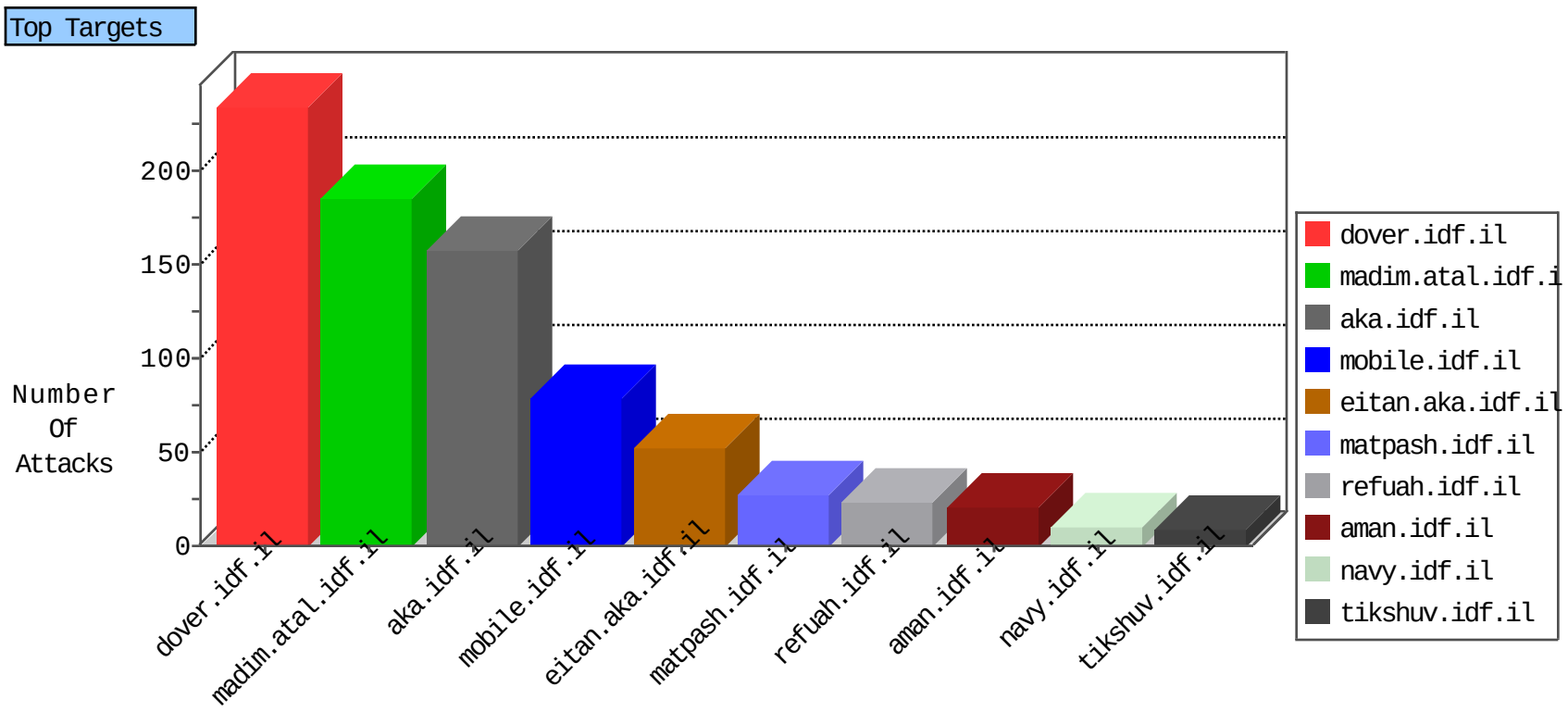
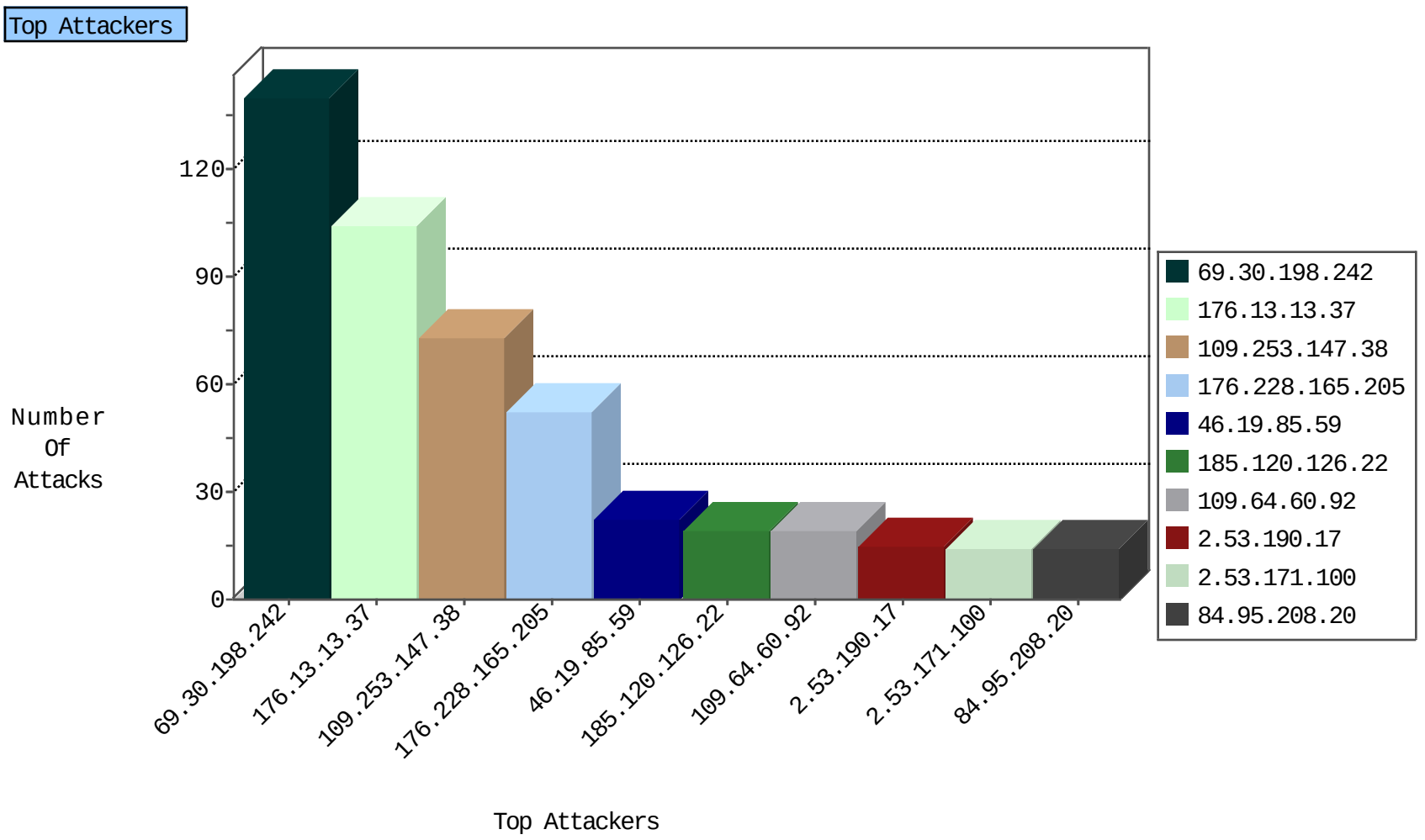
10-01-2016-18:04:05 to 10-01-2016-19:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-01-2016-18:04:05 to 10-01-2016-19:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.3.147.100	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.94.235	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1

10-01-2016-18:04:05 to 10-01-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	123
23.91.70.43	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	6
137.117.9.67	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
137.117.9.67	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
104.223.91.234	United States	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2

10-01-2016-18:04:05 to 10-01-2016-19:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
137.117.9.67	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
23.91.70.43	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
109.67.239.218	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
109.67.239.218	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
179.43.144.21	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.21	147.237.0.35	Switzerland	akaws.idf.il	ET SCAN Potential SSH Scan	1
69.65.95.155	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.72.156	Kenya	aman.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
194.106.139.19	147.237.77.227	Ireland	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
14.152.59.11	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.21	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.21	147.237.76.148	Switzerland	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
139.167.28.125	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.72.53.188	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.121.139.43	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
194.106.139.19	147.237.77.227	Ireland	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
192.169.7.91	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

10-01-2016-18:04:05 to 10-01-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.228.165.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
185.120.126.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.53.190.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.158.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
80.246.137.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.171.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.60.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
172.58.110.201	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.207.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.11.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
69.30.198.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
58.11.68.185	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.64.60.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
174.94.84.65	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.106	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
66.102.9.159	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.155	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.152.202	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.43.74.238	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.231	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.152.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.27	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
87.68.4.255	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.120.126.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
141.226.218.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	3
109.64.60.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.79	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.107.3.125	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.43.204.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.115.224.210	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.108.16.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.147.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2

10-01-2016-18:04:05 to 10-01-2016-19:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.147.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
176.13.19.58	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
2.53.190.17	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.138.69.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	3
2.53.171.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
69.65.95.155	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
2.53.171.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
69.65.95.155	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/matash/login/	Block	2
109.253.158.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
92.187.237.222	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.207.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
180.76.15.149	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
93.158.152.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
69.65.95.155	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.116.77.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
173.231.185.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/i18n/readme.txt	Block	1
82.166.240.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
37.26.149.230	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.120.126.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.239.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
77.124.12.208	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.65.135	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
176.13.11.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
69.65.95.155	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 69.65.95.155	Block	1
37.142.8.250	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
204.79.180.96	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
79.177.194.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding aI_;fAQ&e>{GbP6@ywx@zx!d/u58^O/QN){GDx1akZ.v{MDZ42FdE_vwL-@_o)3ii;1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
82.102.236.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.76.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/hebrew/html/1	Block	1

10-01-2016-18:04:05 to 10-01-2016-19:04:05