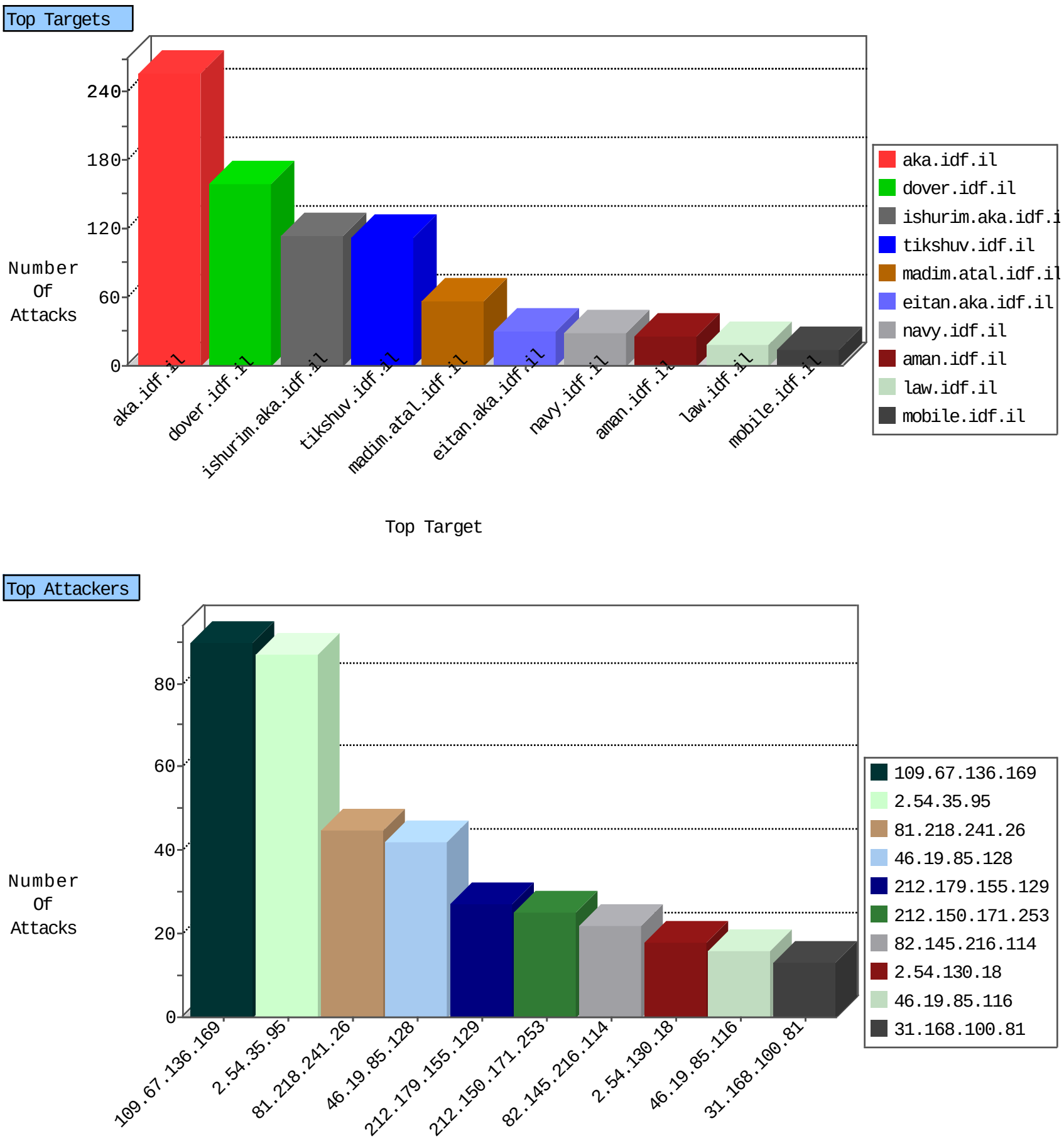
03-08-2016-13:04:08 to 03-08-2016-14:04:08

IDF Under Attack
Daily Report



03-08-2016-13:04:08 to 03-08-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.150.171.253	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
82.145.216.114	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
82.145.216.114	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.52.18.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.240.236.119	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

03-08-2016-13:04:08 to 03-08-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.68.249.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
94.208.145.95	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
94.208.145.95	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.11	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
94.208.145.95	Netherlands	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	1
37.187.94.4	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.183	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
37.187.94.139	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
78.24.34.6	France	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.95.203	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-08-2016-13:04:08 to 03-08-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.45.180.180	147.237.77.19	Spain	law-forum.idf.il	ET SCAN NMAP -sS window 1024	3
79.177.192.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.210.170.165	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
150.70.173.48	147.237.72.166	Japan	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.26.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.212.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.93.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.27.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.143.138.81	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.54.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.217.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
203.186.178.188	147.237.77.74	Hong Kong	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.30	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
152.62.109.208	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.111.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.252.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
13.75.95.104	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
117.247.188.5	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.35.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.160.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.90.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-08-2016-13:04:08 to 03-08-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.136.169	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
2.54.130.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.218	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.179.34.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.210	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
81.218.192.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
212.29.210.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.35.95	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
46.19.85.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.114.23.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.218	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
88.253.43.30	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
31.168.100.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.128.45.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
64.246.165.140	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
46.19.86.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.28.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.59.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.113.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.217.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.54.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.6.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.105.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.123.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.162.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.54.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.67.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-08-2016-13:04:08 to 03-08-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.161.9.12	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
176.13.11.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.161.9.12	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.161.9.12	Block	5
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.9.162	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
193.90.12.89	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
79.178.61.212	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
46.19.86.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.20.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.45.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/870-he/	Block	2
5.197.28.21	Azerbaijan	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
94.230.86.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
80.246.140.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
137.226.113.7	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.143.138.81	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.170.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.99.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.99.17	Block	1
185.82.200.91		147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
95.86.95.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf&sa=u&ved=0ahukewjl_bt2glhlahukjjokhyoxc_cqfggimaa&usg=afqjcnekfq4mo22t0gxa5ab010dusronwg	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
84.108.88.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.88.60	Block	1
212.25.112.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-12980-en/dover.aspx iaf targets terrorist squad that fired a rocket at the erez crossing	Block	1
141.212.122.209	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
85.64.113.65	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
2.52.35.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.99.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/	Block	1
192.243.55.133	Dominica	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/1901.doc	Block	1
46.161.9.12	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
109.64.133.173	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$FAQListViewTemplate1$InternalSearch1$txtFreeTextSearch in www.law.idf.il/338-he/patzar.aspx	Block	1
37.26.146.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.88.60	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
212.76.104.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1292-he/refuah.aspx&sa=u&ved=0ahukewiaxcvrg7hlahuis5okhsgrab4qfgglmae&sig2=rw22nwgm0h8oegjqozglcg&usg=afqjcnfwtc77xg-on-erxerh8xdj1lkm2a	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
149.88.48.178	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
87.71.45.222	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.54.4	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/haredim/general.aspx	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.38.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.146.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.88.60	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
212.76.104.249	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/113270.pdf&sa=u&ved=0ahukewjlvfdshbhlahwnqpokhbz8cnmqfggamac&usg=afqjcnhqkelbu7ci703esjh5hyyba2xlbg	Block	1
46.19.86.215	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.79	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1

03-08-2016-13:04:08 to 03-08-2016-14:04:08