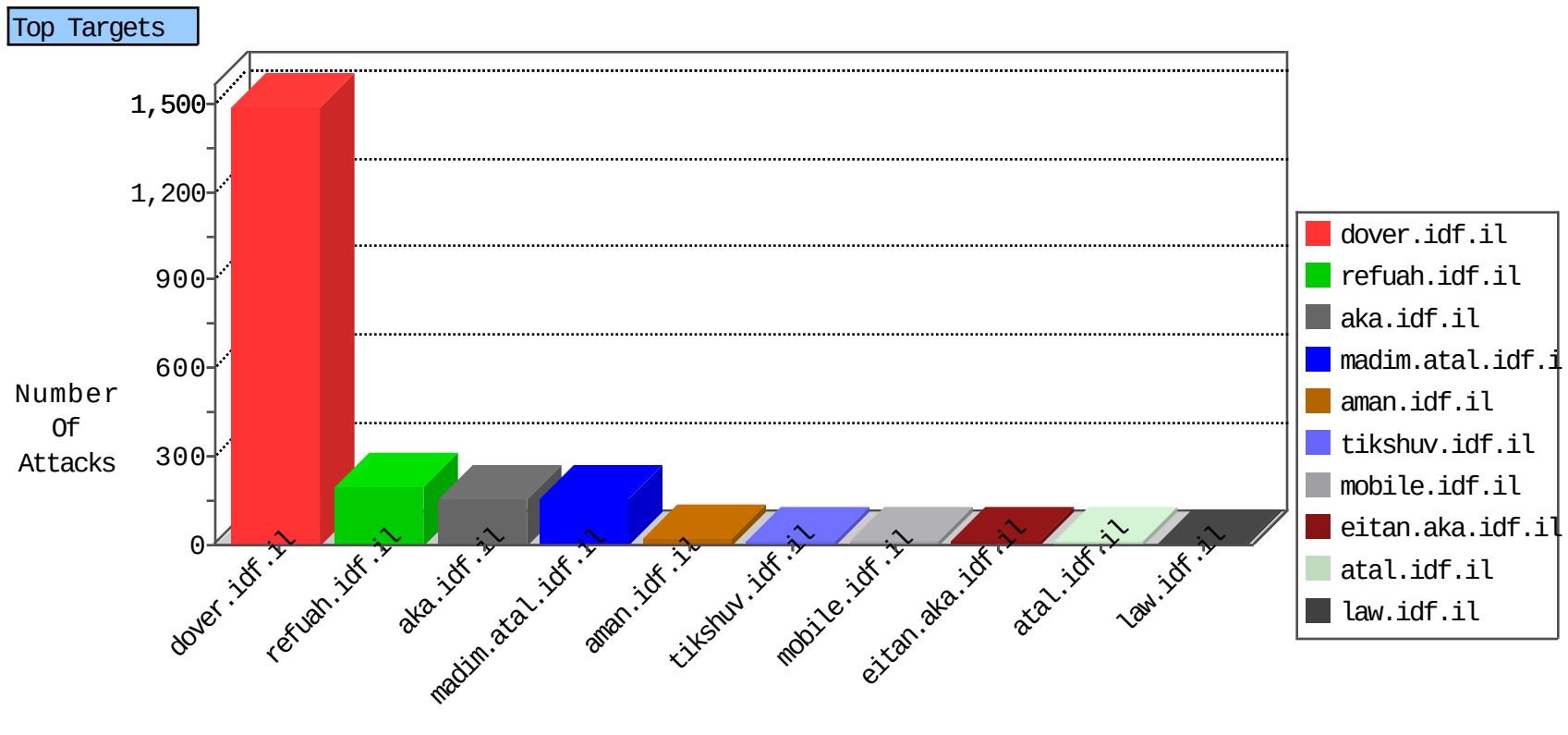
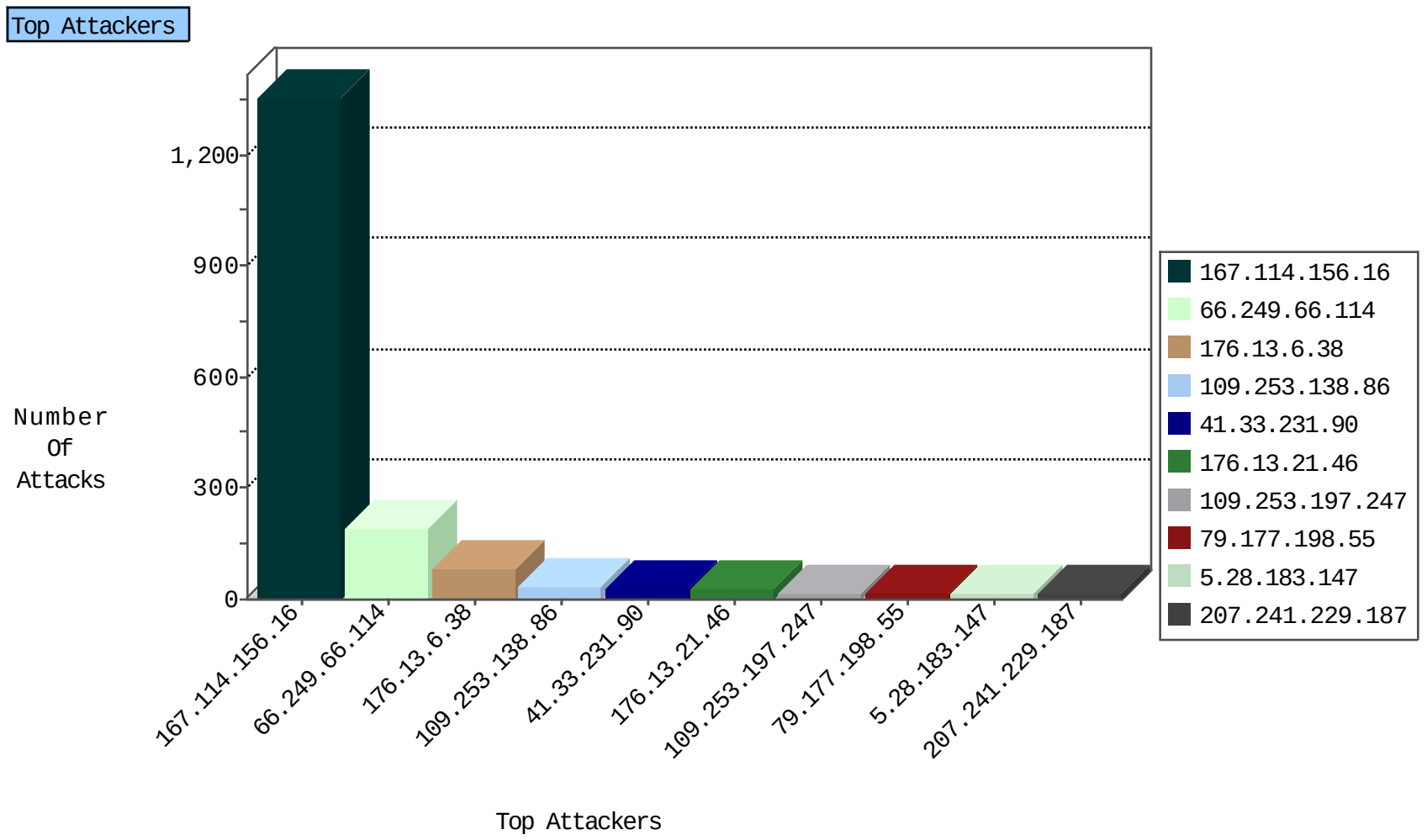
04-15-2016-09:04:04 to 04-15-2016-10:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-15-2016-09:04:04 to 04-15-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1357
134.191.232.71	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	9
101.201.147.32	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	2
184.105.139.94	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
85.25.217.46	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-09:04:04 to 04-15-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
173.234.159.250	United States	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	2
173.234.159.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.76	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
173.234.159.250	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
173.234.159.250	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-09:04:04 to 04-15-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.114	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	188
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.88	147.237.76.196	Lithuania	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.8.14	Lithuania	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.18	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
87.229.116.42	147.237.76.42	Hungary	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
68.116.21.226	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.221	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.88	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.18	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.234	Canada	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.221	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.221	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.88	147.237.77.19	Lithuania	law-forum.idf.il	ET SCAN Potential SSH Scan	1

04-15-2016-09:04:04 to 04-15-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.253.197.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
207.241.229.187	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
79.176.48.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.198.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.76.114.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.28.183.147	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.110.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.50.9.5	Israel	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.53.48.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.182.134.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.153.118	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.198.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.182.134.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.182.134.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.177.198.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.153.118	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.9.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.132.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.181.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.181.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.147.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.45.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.149.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.130.130.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.162.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.53.149.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.163.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
2.55.48.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.149.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.183.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
62.219.162.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
213.8.204.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.53	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.181.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.215	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.130.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.197.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
69.117.245.119	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.28.183.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
109.253.138.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
176.13.21.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
37.26.146.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
93.226.159.130	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
87.71.45.12	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.71.45.12	Block	3
80.246.133.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.180.185	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
188.143.232.123	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 188.143.232.123	Block	1
122.166.172.36	India	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
87.71.45.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/documenttemplates/opgeneralmobile/2088/11334	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
203.127.96.233	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.200.209.212	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
219.74.166.227	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.143.232.123	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
89.139.46.173	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
203.127.96.244	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
219.74.166.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 82.81.2.165 (Open Mode)	None	1
199.30.25.134	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.193.51.81	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-6958-en/patzar.	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
207.46.13.48	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/styles/giyusmaster	Block	1
180.76.15.32	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.81.2.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
203.127.58.228	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.204	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
213.254.241.7	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
68.41.54.48	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
184.172.172.26	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/wp-admin/	Block	1
122.166.172.36	India	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19781-he/dover.aspx	Block	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.2.175	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
107.200.209.212	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
219.74.35.186	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.126.235.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1

04-15-2016-09:04:04 to 04-15-2016-10:04:04