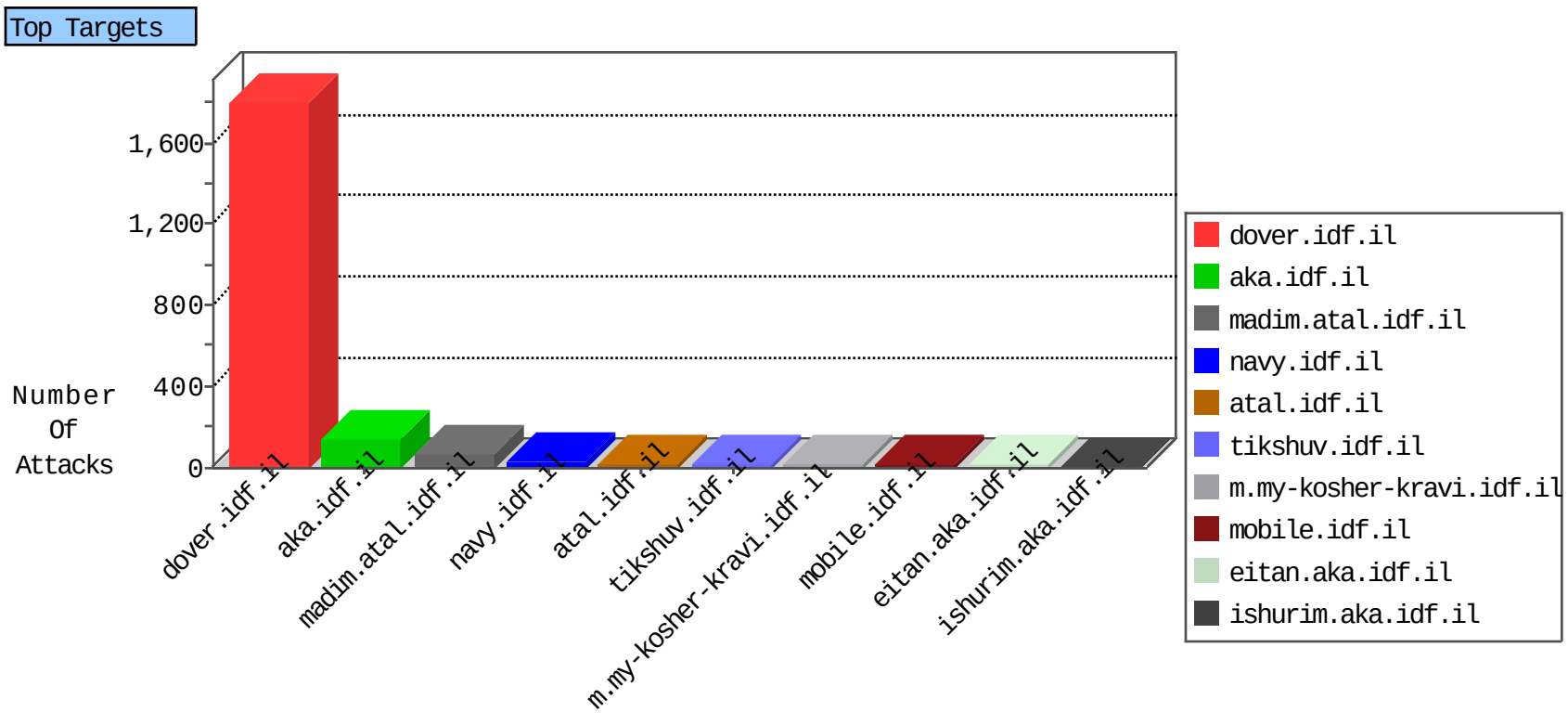
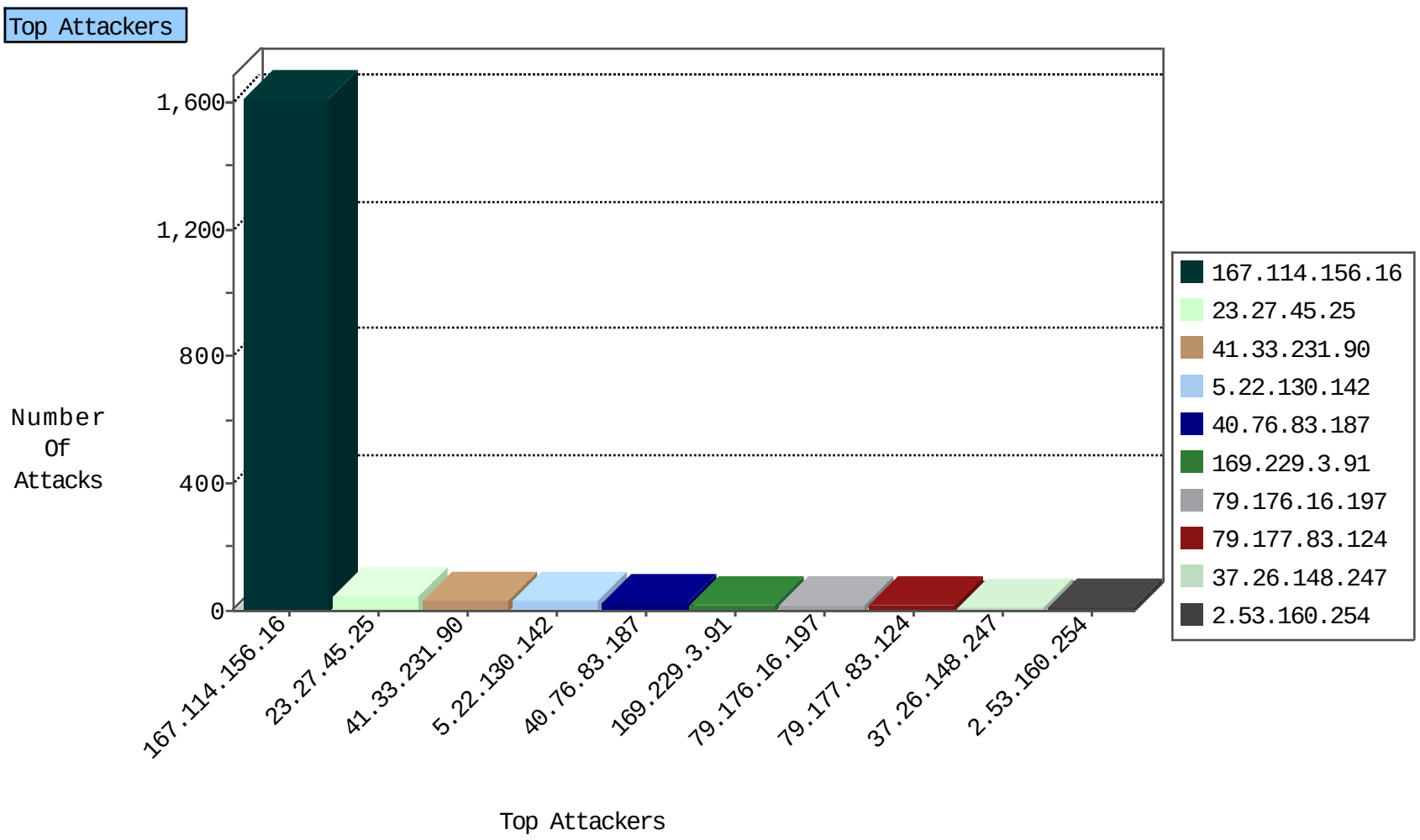
04-15-2016-12:04:09 to 04-15-2016-13:04:09

IDF Under Attack Daily Report





04-15-2016-12:04:09 to 04-15-2016-13:04:09

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	1612
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
220.167.100.13	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1

04-15-2016-12:04:09 to 04-15-2016-13:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.76.83.187	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
40.76.83.187	United States	147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
40.76.83.187	United States	147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
69.30.234.2	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
84.109.241.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.234.2	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.123.172	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.154	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
69.30.234.2	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.123.172	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
40.76.83.187	United States	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
69.30.234.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.234.2	United States	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.123.172	Germany	147.237.0.34	tikshuv.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
40.76.83.187	United States	147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.76.83.187	United States	147.237.76.39	mobile.meitav.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.184	France	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.23	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-15-2016-12:04:09 to 04-15-2016-13:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.128.96	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	10
40.76.83.187	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
195.154.54.169	147.237.72.14	France	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.31.135	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.201.236.155	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
40.76.83.187	147.237.76.39	United States	mobile.meitav.idf.il	ET WEB_SERVER Muieblackcat scanner	1
198.144.184.120	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
52.8.82.27	147.237.77.235	United States	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
40.76.83.187	147.237.76.30	United States	himush.idf.il	ET WEB_SERVER Muieblackcat scanner	1

04-15-2016-12:04:09 to 04-15-2016-13:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
23.27.45.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
2.53.160.254	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.197.120.163	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
79.176.16.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.176.16.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.53.32.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.233.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.11.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.248.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.177.83.124	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
176.13.3.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.216.253	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.83.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
79.177.83.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.29.180.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
141.0.15.32	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.39.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.32.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.124.24.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.147.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.167.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.223.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.53.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.142.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.144.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.182.235.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.4.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.24.73.239	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.45.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.103.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.129.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.102.254.141	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.110.144.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-15-2016-12:04:09 to 04-15-2016-13:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.3.147.121	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-15-2016-12:04:09 to 04-15-2016-13:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.130.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
37.26.148.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
2.53.16.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
195.182.151.246	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
149.78.192.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.142.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.239.224.35	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
107.170.22.185	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 107.170.22.185	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20387-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Malformed URL	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/piwik.php	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/882.pdf	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
46.116.55.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.24.197	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 5.29.24.197 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.64.233.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/drushimw	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
149.88.3.7	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
89.139.9.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method 0ö.Ã¹½¶[[#15]]ðÈ[[#1]]•Ï	Block	1
52.8.82.27	United States	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.255.253.10	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-6967-he/patzar.aspx.	Block	1
207.46.13.140	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
157.55.39.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL	Block	1
31.172.191.231	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
128.232.110.28	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
217.69.136.208	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.75.6	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
157.55.39.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.188	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
2.55.4.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
107.170.22.185	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
189.218.226.123	Mexico	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

04-15-2016-12:04:09 to 04-15-2016-13:04:09