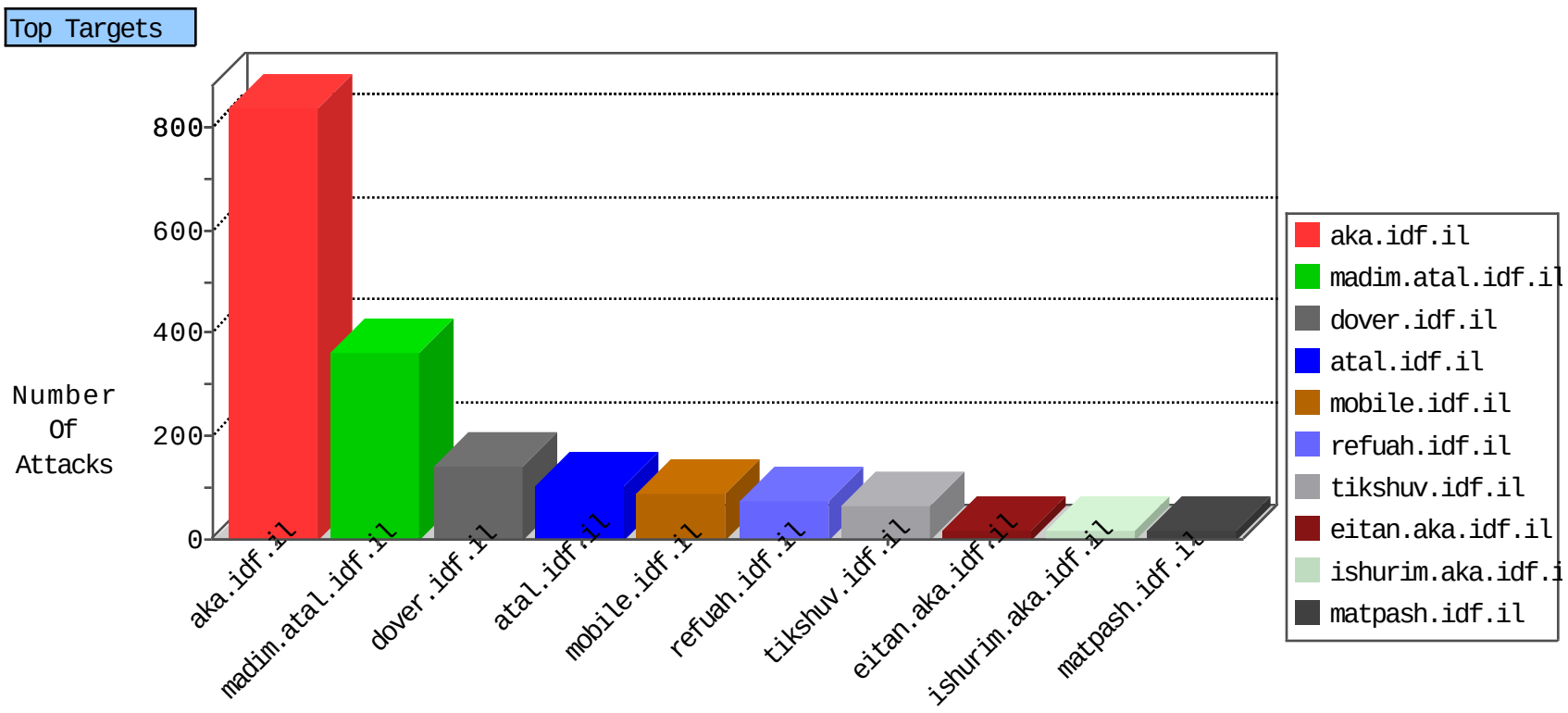
02-29-2016-14:04:02 to 02-29-2016-15:04:02

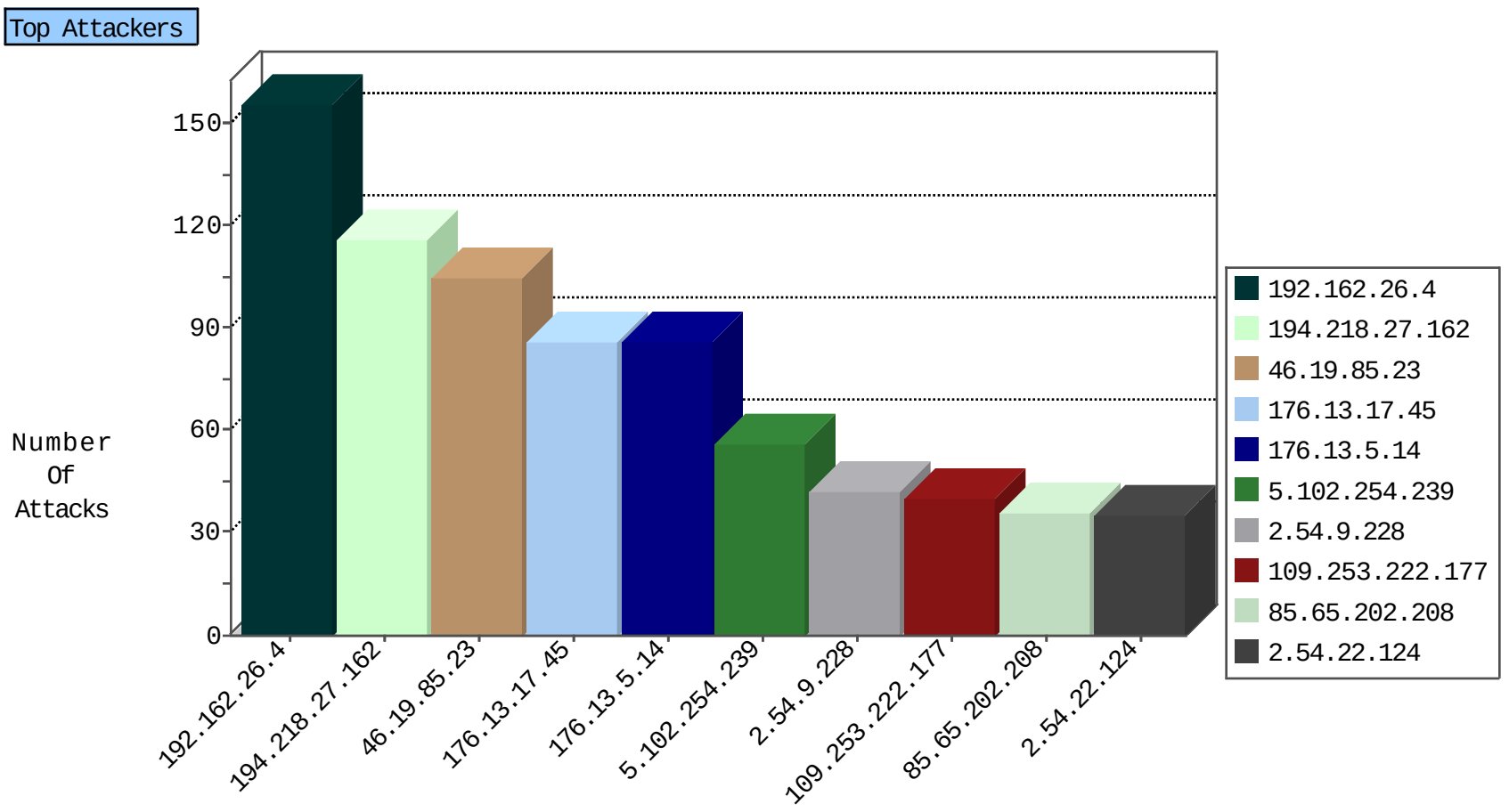
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-29-2016-14:04:02 to 02-29-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.219.83	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
185.130.5.196		147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
193.242.218.6	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.196		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-14:04:02 to 02-29-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
62.219.131.177	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
109.67.41.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.250.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
104.255.65.207		147.237.76.200	eitan.aka.idf.il	0543: HTTP: php.cgi Access	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	147.237.77.176	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

02-29-2016-14:04:02 to 02-29-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.194.196.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.104.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.188.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.140.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.27.45.139	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.104.77.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.195.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.142.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.199.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
136.243.130.9	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.75.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
136.0.99.139	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.43.73.129	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
105.156.121.186	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.32.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.143.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.200.142.180	147.237.72.156	Kazakstan	aman.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.226.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.163.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.133.88	147.237.77.216	Israel	dover.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
80.179.11.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.166.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.51.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.58.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
136.243.130.9	147.237.76.201	Germany	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.1.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.134.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.79.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-29-2016-14:04:02 to 02-29-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	76
5.102.254.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	40
109.253.222.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
2.54.56.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.253.219.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
37.142.196.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
85.65.202.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
192.118.78.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.22.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
213.8.38.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
109.253.219.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
185.120.125.38		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.213.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.65.202.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	12
5.102.254.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
178.214.79.116	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
80.246.133.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
62.219.135.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
105.106.143.247	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
178.214.79.116	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.168.96.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.177.235.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
64.120.16.196	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.57.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.147.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
84.94.223.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.4.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.125.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.64.94.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.28.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.65.202.208	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.37.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.166.123	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
147.236.50.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.64.71.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
209.88.157.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.22.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

02-29-2016-14:04:02 to 02-29-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
176.13.5.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.17.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.54.9.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.46.38.188	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.46.38.188	Block	13
31.210.186.249	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.210.186.249	Block	12
109.253.222.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	7
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	7
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	7
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	7
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 192.162.26.4	Block	6
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 192.162.26.4	Block	6
31.210.186.249	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
37.46.38.188	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 192.162.26.4	Block	6
2.54.56.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
62.219.254.97	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	5
89.234.157.254	France	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 89.234.157.254	Block	5
176.12.160.1	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	5
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 192.162.26.4	Block	5
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 192.162.26.4	Block	5
84.94.179.12	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.179.12	Block	5
66.249.64.207	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	4
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.125.109.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.109.68	Block	4
66.249.64.202	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	4
134.249.65.86	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
109.226.17.214	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.206.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.46.38.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.119.127.64	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
84.94.179.12	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
109.253.146.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 192.162.26.4	Block	3
37.46.38.185	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
109.253.205.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.125.109.68	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.52.141.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
176.13.6.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1

02-29-2016-14:04:02 to 02-29-2016-15:04:02