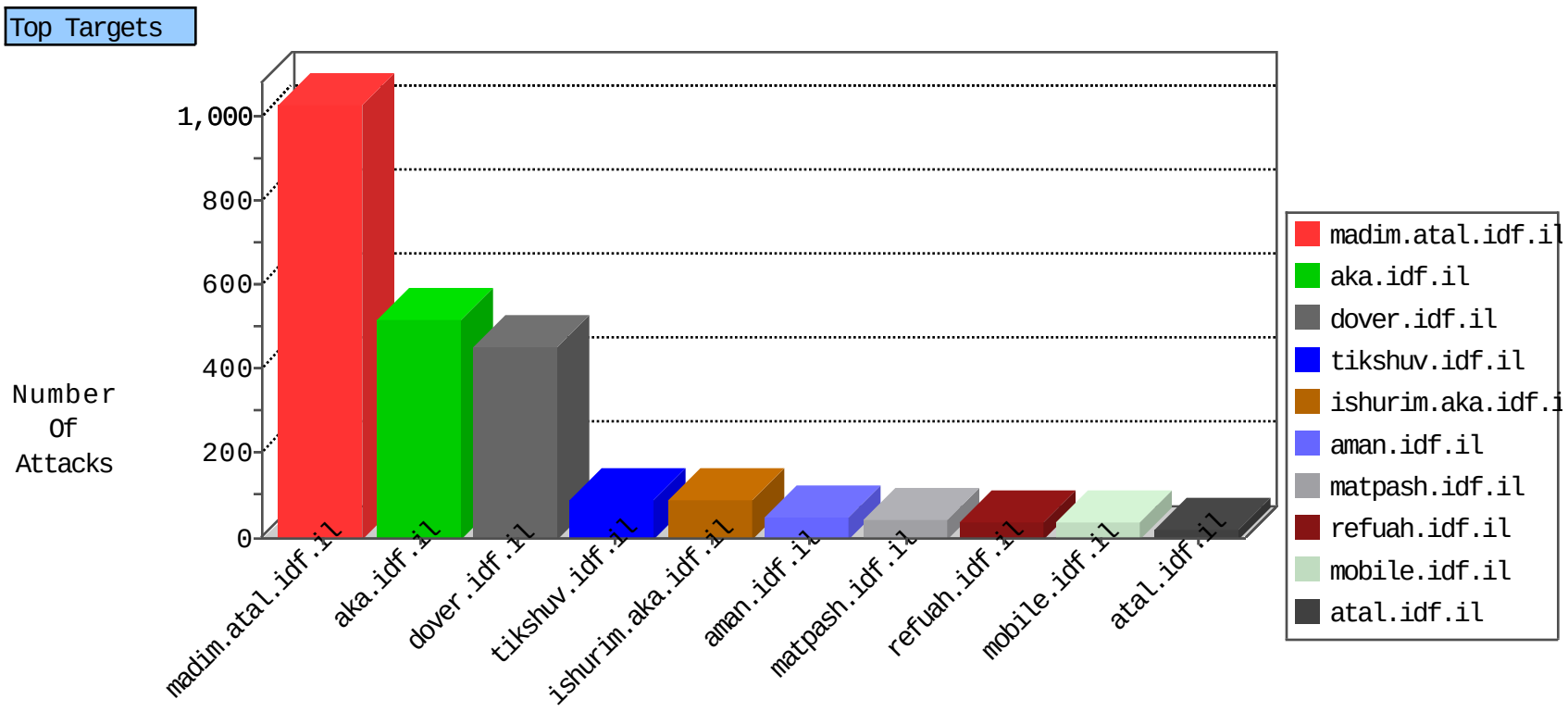
02-22-2016-12:04:07 to 02-22-2016-13:04:07

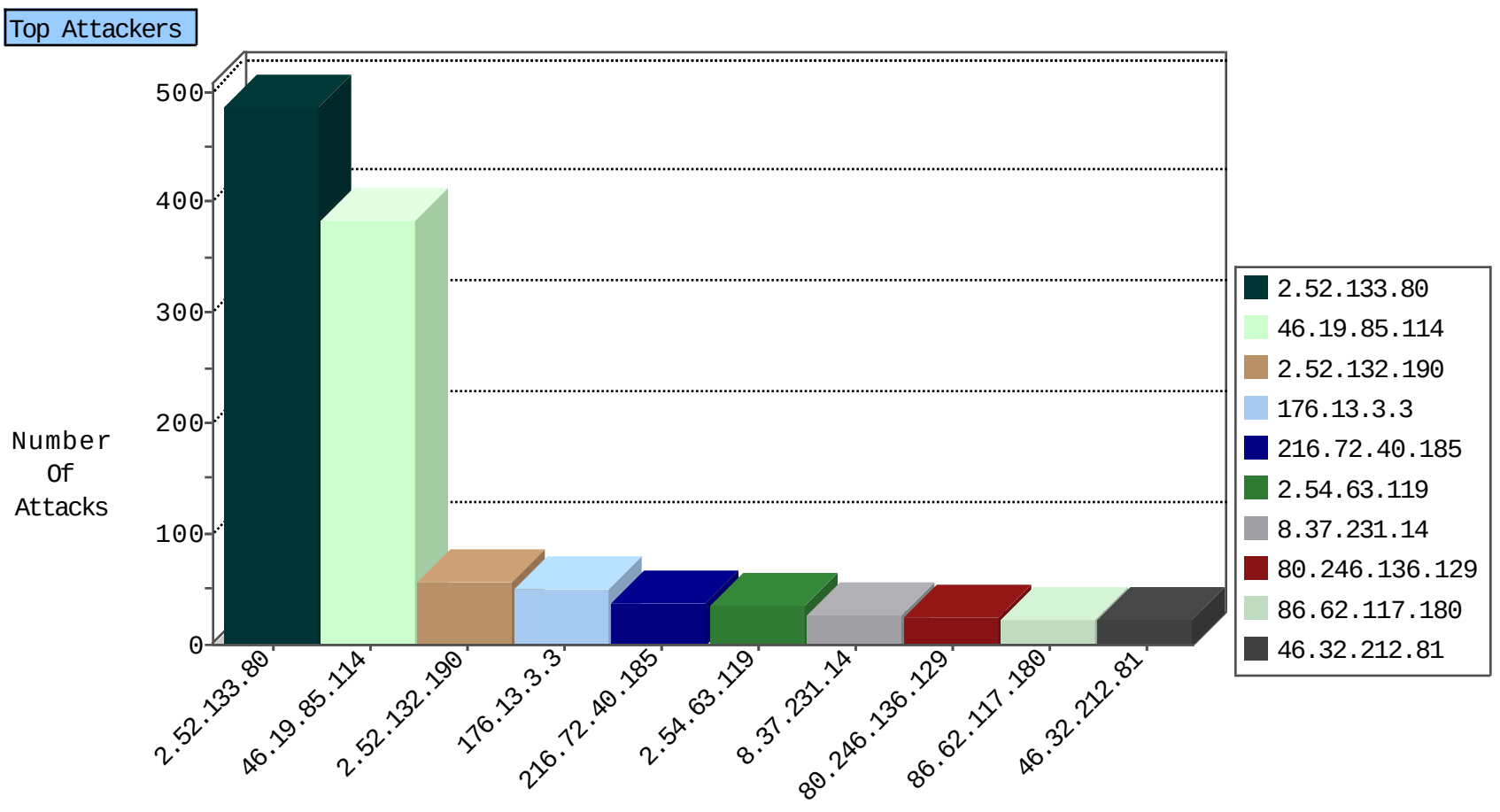
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-22-2016-12:04:07 to 02-22-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	45
213.57.88.74	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.231.14	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
107.150.60.75	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1

02-22-2016-12:04:07 to 02-22-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.132.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
217.132.152.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	10
31.168.144.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
87.71.161.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
69.30.213.18	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
188.40.95.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.213.18	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
79.179.52.186	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.219.239.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.40.95.70	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.39.60.187	China	147.237.77.179	e.mazi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
79.181.146.91	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

02-22-2016-12:04:07 to 02-22-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.29.139	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
80.246.136.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.183.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.162.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.8.4	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
192.117.129.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.235.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.157.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.107	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.76.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.115.113.89	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.25.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-22-2016-12:04:07 to 02-22-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.14	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
46.32.212.81	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
2.52.132.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.147.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
5.57.20.129	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
176.13.23.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.254.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
84.95.202.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
81.218.195.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
109.67.7.244	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.57.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.102.9.65	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
2.52.164.111	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.161.51	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.179.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.207.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
194.90.251.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
94.27.207.217	Hungary	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.228.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.170.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.25.102.63	Israel	147.237.76.198	e.yohalan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.131.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.230.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.171.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.209.177.95	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.4.198	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.207.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
81.209.177.189	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
194.90.251.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.136.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
45.55.53.138		147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.136.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

02-22-2016-12:04:07 to 02-22-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.133.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	311
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
2.52.133.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	176
46.19.85.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
176.13.3.3	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.3.3	Block	51
2.52.132.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.54.63.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.72.40.185	Block	24
2.54.130.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.54.139.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	12
86.62.117.180	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	12
86.62.117.180	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 86.62.117.180	Block	10
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.65.115.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.65.115.231	Block	6
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	6
2.54.130.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.52.132.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.147.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
82.81.20.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	4
109.65.115.231	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
81.209.177.95	Europe	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 81.209.177.95	Block	4
185.89.217.232		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.89.217.226		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
109.253.206.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.120.134.161	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	3
109.253.141.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.158	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
41.102.230.200	Algeria	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 41.102.230.200 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
91.199.69.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	2
213.151.48.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewii-kxxk4vlahuceywkhrbcai8qfggnmaa&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	2
109.253.131.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
78.137.0.115	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	2
83.166.234.6	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	2
46.117.98.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.81.20.169	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
79.179.221.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	2
109.64.124.236	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
199.30.24.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.13.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
213.57.39.182	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	2

02-22-2016-12:04:07 to 02-22-2016-13:04:07