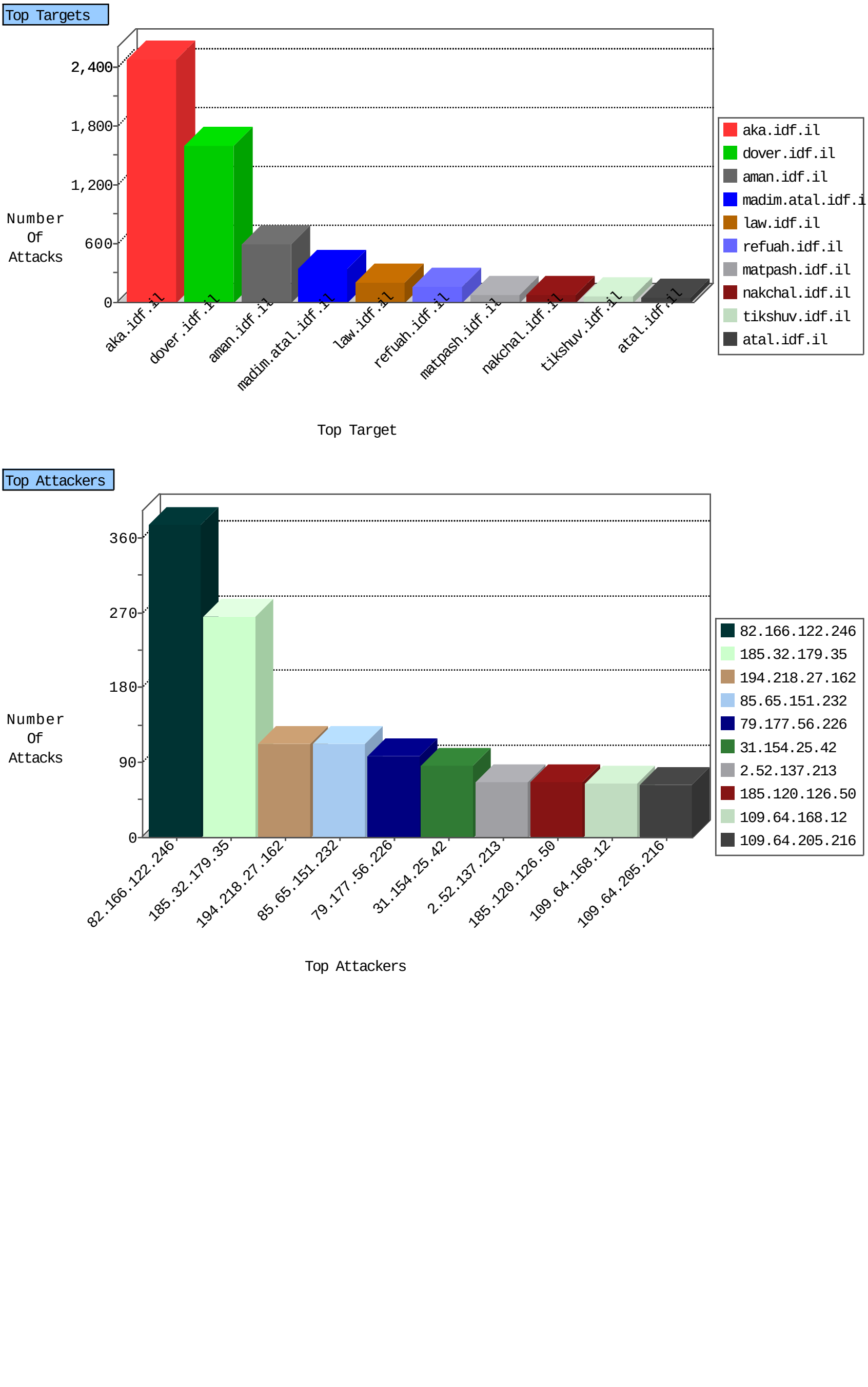
02-14-2016-23:04:08 to 02-15-2016-00:04:08

IDF Under Attack Daily Report



02-14-2016-23:04:08 to 02-15-2016-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.138.17.205	France	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

02-14-2016-23:04:08 to 02-15-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-14-2016-23:04:08 to 02-15-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.91	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	24
185.32.179.35	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.176.165.67	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.230	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
119.81.162.182	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.51.30	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.122.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.182.242.200	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
79.182.168.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.148	United States	gqcenter.aka.idf.il	ET DROP Dshield Block Listed Source	1
45.32.39.185	147.237.0.33		idf.il	ET SCAN NMAP -sS window 3072	1
119.81.162.182	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.39.185	147.237.0.33		idf.il	ET SCAN NMAP -f -sS	1
119.81.162.182	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.193	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
83.87.96.168	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.182.242.200	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.177.213.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.25	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
177.246.199.209	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.39.185	147.237.0.33		idf.il	ET SCAN NMAP -sS window 2048	1

02-14-2016-23:04:08 to 02-15-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	284
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	59
79.67.165.140	United Kingdom	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	53
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
85.65.151.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
176.13.16.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.65.151.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
79.177.56.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	33
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	32
79.177.56.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	32
85.65.151.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
31.210.186.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
83.130.109.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
87.68.151.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
83.130.109.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
40.77.167.26	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
2.52.137.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
172.13.166.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	25
37.46.39.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
40.77.167.26	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
46.19.86.4	Israel	147.237.76.31	nakchal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.68.151.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
2.52.137.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
157.55.39.165	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
157.55.39.165	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
172.13.166.38	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
185.120.126.50		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
5.22.134.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
109.67.188.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
185.120.126.50		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	20
109.67.188.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
109.64.168.12	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
37.26.146.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
109.64.17.116	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
37.26.146.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
79.179.121.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
81.218.204.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
89.138.78.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
84.108.216.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.179.173.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.177.56.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
79.179.121.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
109.64.17.116	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17

02-14-2016-23:04:08 to 02-15-2016-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	130
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 185.32.179.35	Block	22
79.176.203.35	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.176.203.35	Block	7
79.176.203.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
79.179.121.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.83.3	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
109.253.208.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$datepicker1 in www.idf.il/1153-he/dover.aspx	Block	3
31.210.189.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.124.118	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.106.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.181.229.82	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
93.172.187.52	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.136.2	Block	2
79.180.34.35	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
176.13.16.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
84.111.180.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
5.29.157.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
94.159.156.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.160.112	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
5.29.182.95	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.120.219.12	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.179.3.248	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
93.172.182.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
109.253.205.116	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.121.68.210	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
213.8.204.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
89.138.76.255	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
69.248.129.181	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
149.78.58.52	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
31.210.189.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.111.110.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.94.187.174	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
213.151.37.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mailbox.aspx&sa=u&ved=0ahukewj9gto5m_jkahvccpokhc4fcawqjbaicg&usg=afqjcnfw8xbjdj46aa_ieeng07gs79p8hq	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
109.67.251.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
5.22.135.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
2.54.6.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
199.30.16.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.46.39.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1

02-14-2016-23:04:08 to 02-15-2016-00:04:08