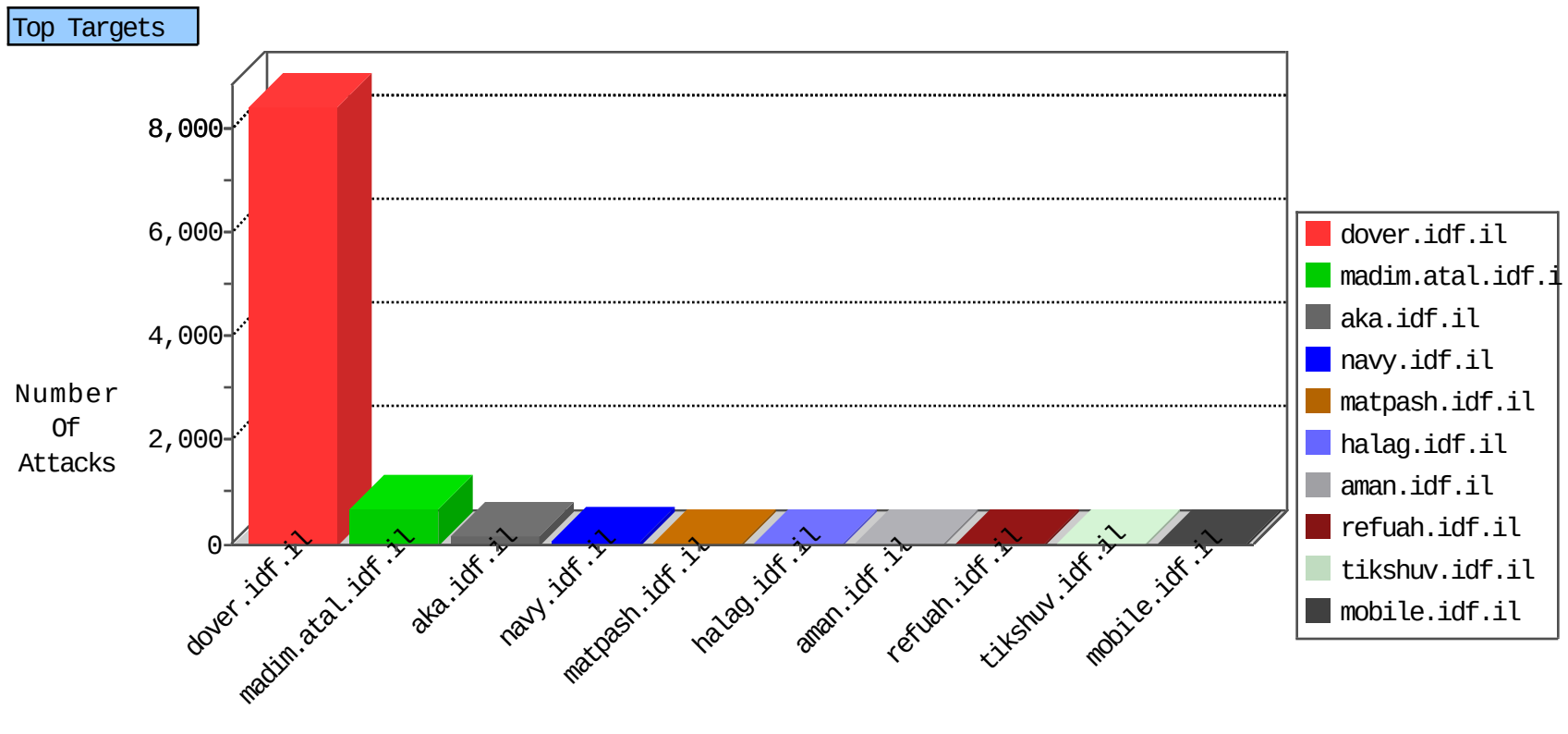
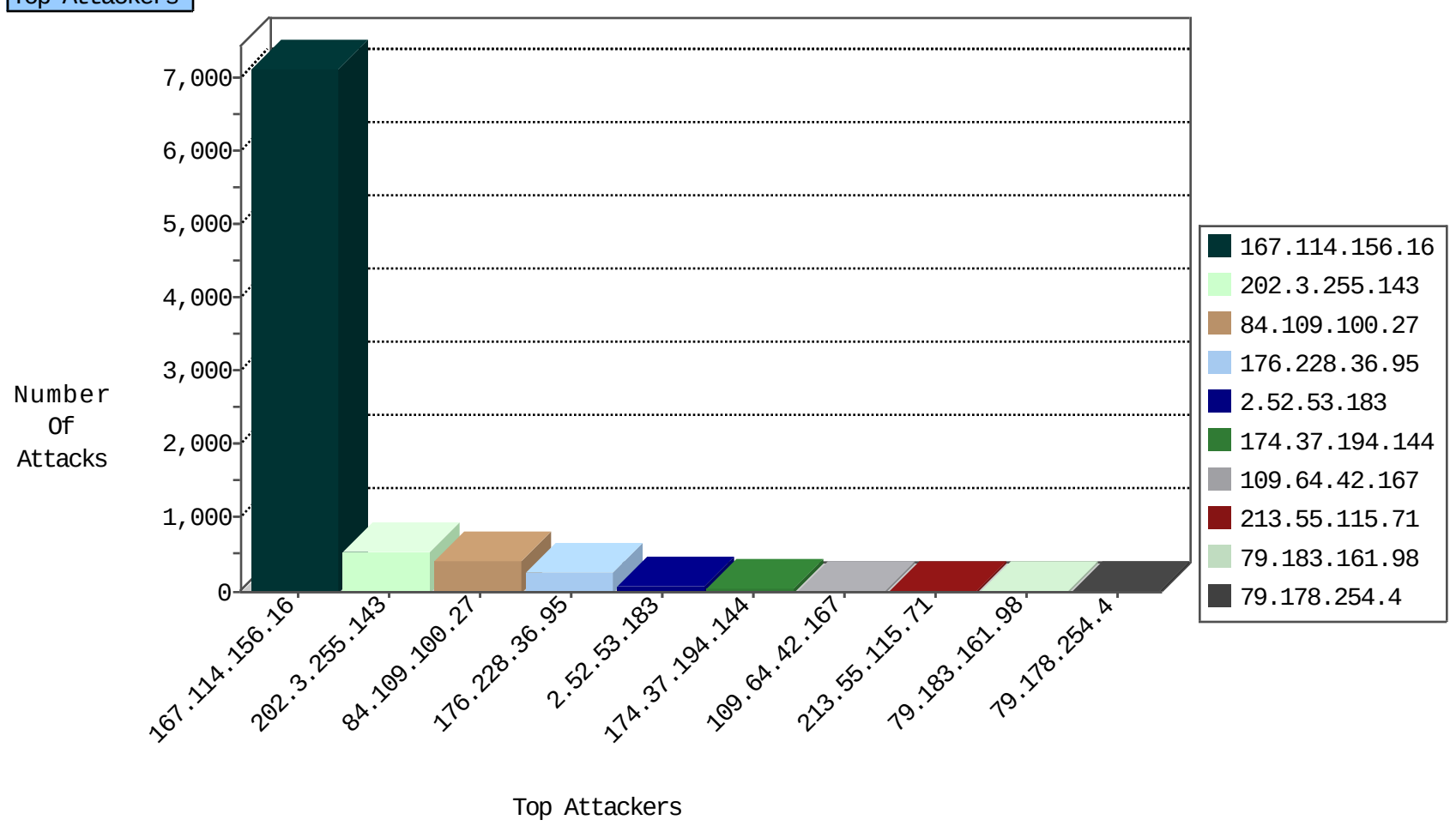
01-15-2016-08:04:08 to 01-15-2016-09:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-15-2016-08:04:08 to 01-15-2016-09:04:08

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	DOS-Tool-SwitchbladG	dest-reset	2759
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
222.245.118.143	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
14.114.251.37	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
14.114.251.37	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
14.114.251.37	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

01-15-2016-08:04:08 to 01-15-2016-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-15-2016-08:04:08 to 01-15-2016-09:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	510
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
174.37.194.144	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sA (2)	2
37.48.65.40	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	2
192.3.176.150	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
85.65.149.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.0.200	India	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
84.228.47.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.0.200	India	m4u.idf.il	ET SCAN NMAP -f -sS	1
78.184.196.99	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
67.231.20.97	147.237.76.34	Canada	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.21.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
174.37.194.144	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
208.52.161.177	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Setup.php access	1
46.19.85.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.48.65.40	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
192.3.176.150	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
106.38.241.106	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
183.131.19.18	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.171.2	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
183.82.106.200	147.237.0.200	India	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
84.94.57.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
71.6.165.200	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
67.231.20.97	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
115.236.75.201	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.40	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
192.3.176.150	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
114.112.90.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

01-15-2016-08:04:08 to 01-15-2016-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3986
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3000
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
109.64.42.167	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
79.183.161.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.55.115.71	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.52.53.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.52.53.183	Israel	147.237.76.86	navy.idf.il	SYN Attack		reject	16
192.117.138.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.178.254.4	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.15	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.178.254.4	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
2.52.53.183	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
2.52.53.183	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.134.57	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.53.183	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.53.183	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.115.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.168.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.176	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
46.19.86.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.43.41.57	Bulgaria	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.13.112.122	Ireland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
84.109.100.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
131.253.25.166	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
173.252.89.225	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.99.32.2		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.67.103.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.60.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.99	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	3
46.19.86.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.174.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.52.161.177	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
79.177.148.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.38.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.148	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	3
2.54.170.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.37.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-15-2016-08:04:08 to 01-15-2016-09:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.109.100.27	Block	289
176.228.36.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
176.228.36.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.6.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.109.100.27	Block	6
79.183.97.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
85.64.128.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.212.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.33.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.49.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.5.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
109.253.193.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.71	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
46.121.69.156	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.147.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.160.178.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.109.100.27	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
79.183.186.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.52.161.177	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /mysql/scripts/setup.php	Block	1
157.55.39.174	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/sckjksdcfksdshitjfsl.aspx	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.186.93.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.178.101.40	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.163	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.42.167	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.109.100.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
66.249.93.103	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/infocenteritem/browser.png	Block	1
183.15.4.140	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method qv1 in URL	Block	1
88.73.9.247	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an	Block	1
2.54.52.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
80.178.204.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/tfasim.gif	Block	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
109.65.220.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-15-2016-08:04:08 to 01-15-2016-09:04:08