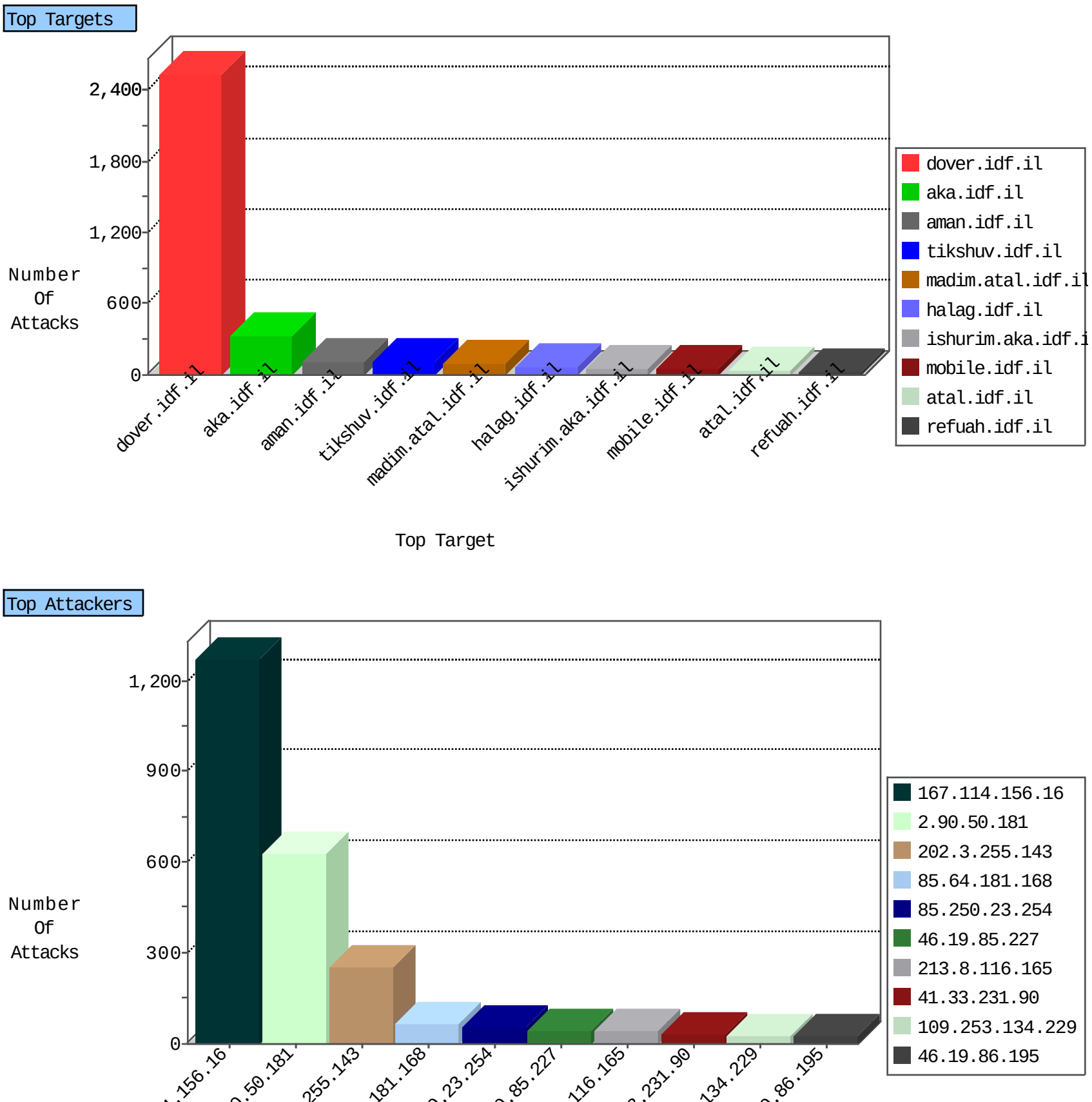
01-17-2016-16:04:09 to 01-17-2016-17:04:09

IDF Under Attack
Daily Report



01-17-2016-16:04:09 to 01-17-2016-17:04:09

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	DOS-Tool-SwitchbladG	dest-reset	3000
2.52.52.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.181.12.59	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
80.246.130.175	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.54.237	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
151.80.109.172	Italy	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-17-2016-16:04:09 to 01-17-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.i	C091: HTTP: Access to - admin.asp	Block	38
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.i	C023: HTTP: administrator in URI	Permit	2
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.i	C003: HTTP: phpMyAdmin access	Block	2
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.i	C015: HTTP: Suspicious Dir Access	Block	2
123.126.113.154	China	147.237.77.216	dover.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-17-2016-16:04:09 to 01-17-2016-17:04:09

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	214
2.90.50.181	147.237.77.216	Saudi Arabia	dover.idf.il	Admin login page scan - Havij	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
2.90.50.181	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP login.htm access	2
2.90.50.181	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP admin.php access	2
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
171.112.96.169	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
85.65.169.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.99	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.161.40.120	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
212.129.55.113	147.237.77.212	France	e.dover.idf.il	ET SCAN Potential SSH Scan	1
5.102.253.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.129.55.113	147.237.76.30	France	himush.idf.il	ET SCAN Potential SSH Scan	1
2.90.50.181	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP adminlogin access	1
204.151.12.168	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
171.112.96.169	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.206.201.94	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.182.144.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.21	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
213.57.104.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.148.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.129.55.113	147.237.76.86	France	navy.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

01-17-2016-16:04:09 to 01-17-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.250.23.254	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
213.8.116.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
149.20.63.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
107.167.108.213	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
79.178.145.119	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
79.182.116.94	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
90.184.141.245	Denmark	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.159.152.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
84.111.155.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
94.159.152.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.189.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.127.182.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.29.175.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
84.108.103.28	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
194.90.66.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.28.179.170	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.12.132.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.126.102		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.105.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.29.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.29	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.187.96	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.179.17.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.62	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.64.157.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
110.168.230.89	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.87.115.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
140.101.20.1	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
94.188.248.67	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.4.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

01-17-2016-16:04:09 to 01-17-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.90.50.181	Block	370
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	105
2.90.50.181	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	98
85.64.181.168	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
109.253.134.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	26
195.244.23.42	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 195.244.23.42	Block	17
46.19.86.131	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	14
140.101.20.1	United States	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.56	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.86.56	None	4
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.189.226	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
109.186.175.4	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.119.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.178.99.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	2
46.120.164.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.253.146.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.172.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.22.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
198.15.125.34	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
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	2
185.3.147.167	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
94.159.152.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.74.38.98	Sweden	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
78.142.173.10	Austria	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
173.254.28.139	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
141.212.122.81	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Malformed URL com.facebook.katana	Block	1
89.161.204.53	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/general.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
186.202.127.122	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
50.62.208.146	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
213.151.36.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113539.pdf&sa=u&ved=0ahukewihlbwghrhkahwbhywkhtbtbroqfggsmas&usg=afqjcnfcsla-ae4x4-hiocx53dp9niqymq	Block	1
37.26.146.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.116.94	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.31.229.182	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
104.238.73.139		147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
92.63.140.212	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
191.252.51.11	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.33	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1

01-17-2016-16:04:09 to 01-17-2016-17:04:09