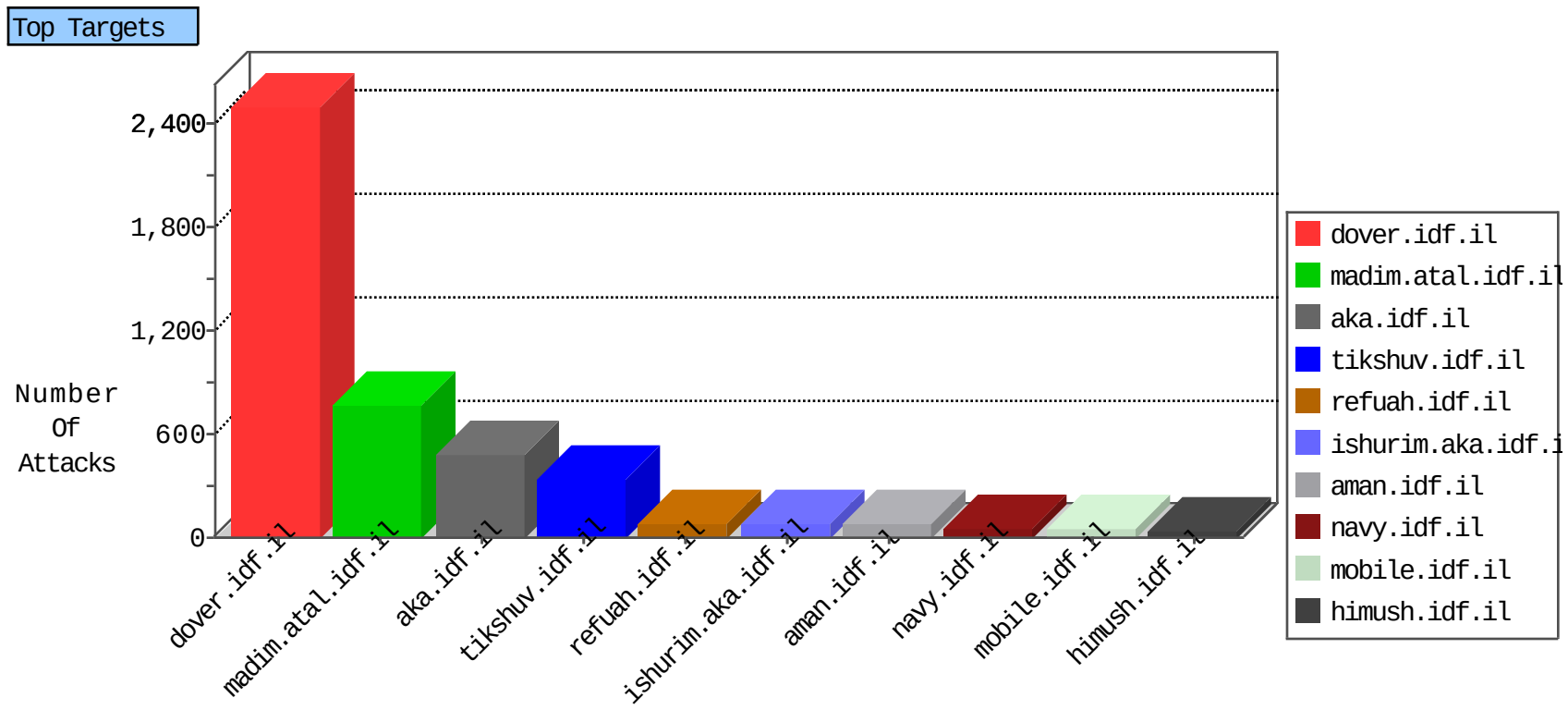
01-18-2016-21:04:03 to 01-18-2016-22:04:03

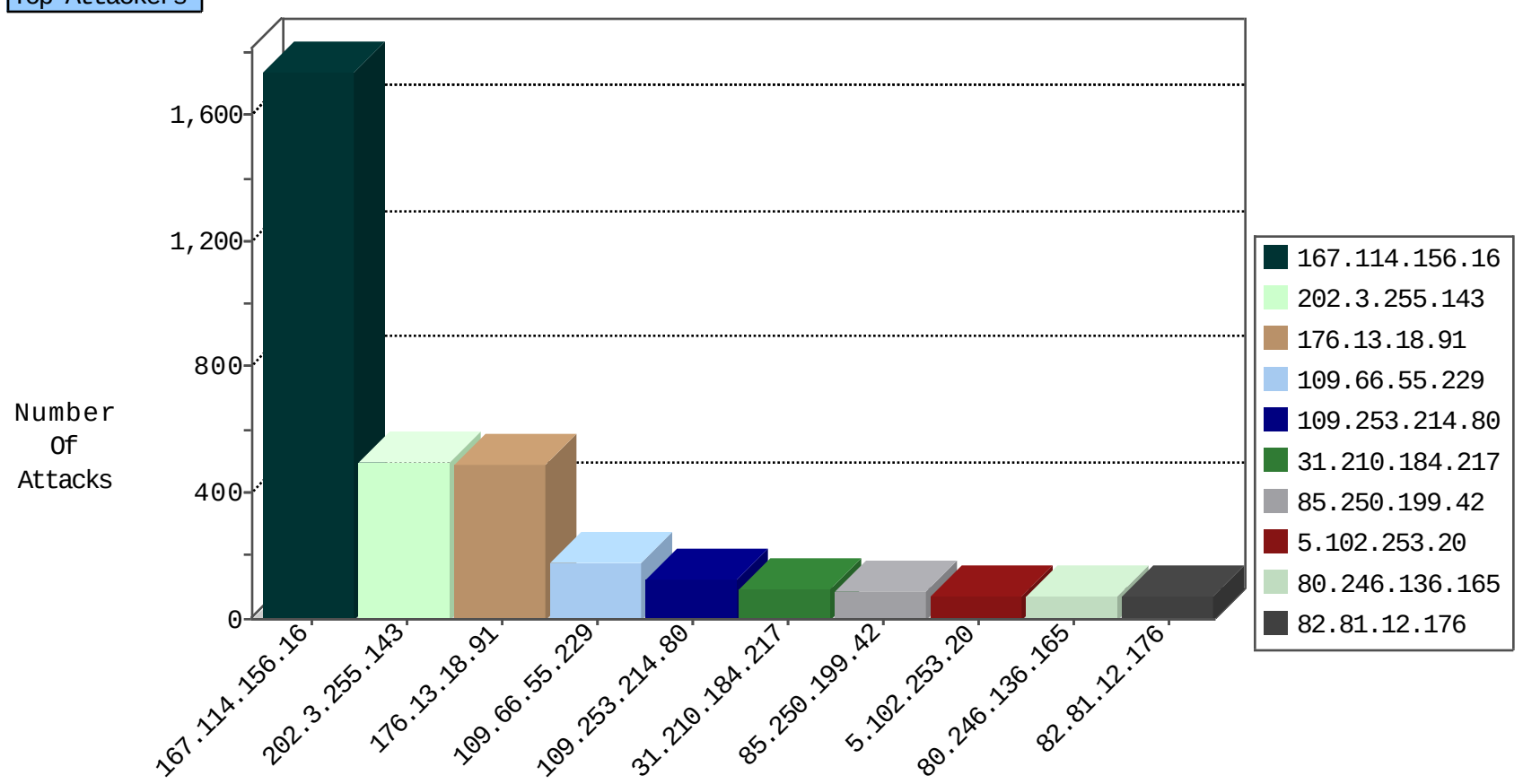
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-18-2016-21:04:03 to 01-18-2016-22:04:03

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
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	70
109.66.99.58	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.152.75	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
142.54.160.213	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
120.56.249.51	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

01-18-2016-21:04:03 to 01-18-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.70	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	13
40.113.8.22	United States	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
40.113.8.22	United States	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	8
37.26.146.234	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
109.66.55.229	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
40.113.8.22	United States	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
10.0.0.2		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	4
40.113.8.22	United States	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
84.108.56.186	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
40.113.8.22	United States	147.237.0.34	tikshuv.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
40.113.8.22	United States	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
188.165.15.26	France	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-18-2016-21:04:03 to 01-18-2016-22:04:03

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	457
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
40.113.8.22	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
40.113.8.22	147.237.0.34	United States	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	2
88.204.187.90	147.237.72.166	Kazakstan	aka.idf.il	ET SCAN NMAP -sS window 4096	1
84.109.50.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.227.141.74	147.237.77.216	Sweden	dover.idf.il	portscan: TCP Distributed Portscan	1
40.113.8.22	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
213.8.204.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.77.243	Cote D'Ivoire	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
132.68.8.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.51.172.34	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.151.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.60.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.181.243.149	147.237.72.166	Finland	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.6.197.169	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.184.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.171.23.126	147.237.76.86	Vietnam	navy.idf.il	ET SCAN Potential SSH Scan	1
91.218.246.103	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

01-18-2016-21:04:03 to 01-18-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.253.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.5.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.178.34.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.102.253.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
85.65.26.192	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
85.65.26.192	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
87.68.39.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.145.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.28.2	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.178.145.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.145.251	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack		reject	11
46.19.85.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.177.115.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.65.186.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.54.37.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.115.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.145.251	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
82.114.168.157	Yemen	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
81.174.152.11	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.116.76.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.192.252	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.174.152.11	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.138.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.45	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
2.54.145.251	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.253.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.45.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.192.252	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
2.54.145.251	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.192.252	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.207.1	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
2.54.145.251	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
196.221.195.136	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.68.37.3	Israel	147.237.76.34	yohalan.idf.il	drop		drop	4
212.143.142.56	Israel	147.237.77.216	dover.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
197.162.22.209	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.98	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
196.217.74.101	Morocco	147.237.77.216	dover.idf.il	drop		drop	4
37.26.147.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence		alert	4
109.253.135.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
197.162.22.209	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

01-18-2016-21:04:03 to 01-18-2016-22:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	277
109.66.55.229	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
109.253.214.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.18.91	Block	106
31.210.184.217	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.210.184.217	Block	90
85.250.199.42	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
80.246.136.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
176.13.11.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
213.8.204.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.226.21.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.179.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.136.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.165	Block	5
31.168.64.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
41.131.102.40	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
41.131.102.40	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	3
109.253.140.148	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
2.54.142.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.90.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.180.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
82.81.29.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.95.221	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/465-he/patzar.aspx&sa=u&ved=0ahukewieo-tkibtkahxh8ywkhei9dmcqfggimaa&sig2=pjsw5pn_oc_crjb1sx29ea&usg=afqjcngqzbh9wiluednjuc5_32bvfk7wuw	Block	2
192.254.139.211	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.5.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
192.254.139.211	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.187.127	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.186.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.115.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.13.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.184.217	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
89.161.178.3	Poland	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
188.121.54.80	Netherlands	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8925-he/refuah.aspx	Block	1
143.95.197.199	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/106902.pdf	Block	1
109.253.135.194	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
207.46.13.105	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
5.100.248.26	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
84.229.30.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.31.229.182	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
108.186.192.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
195.74.38.121	Sweden	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1

01-18-2016-21:04:03 to 01-18-2016-22:04:03