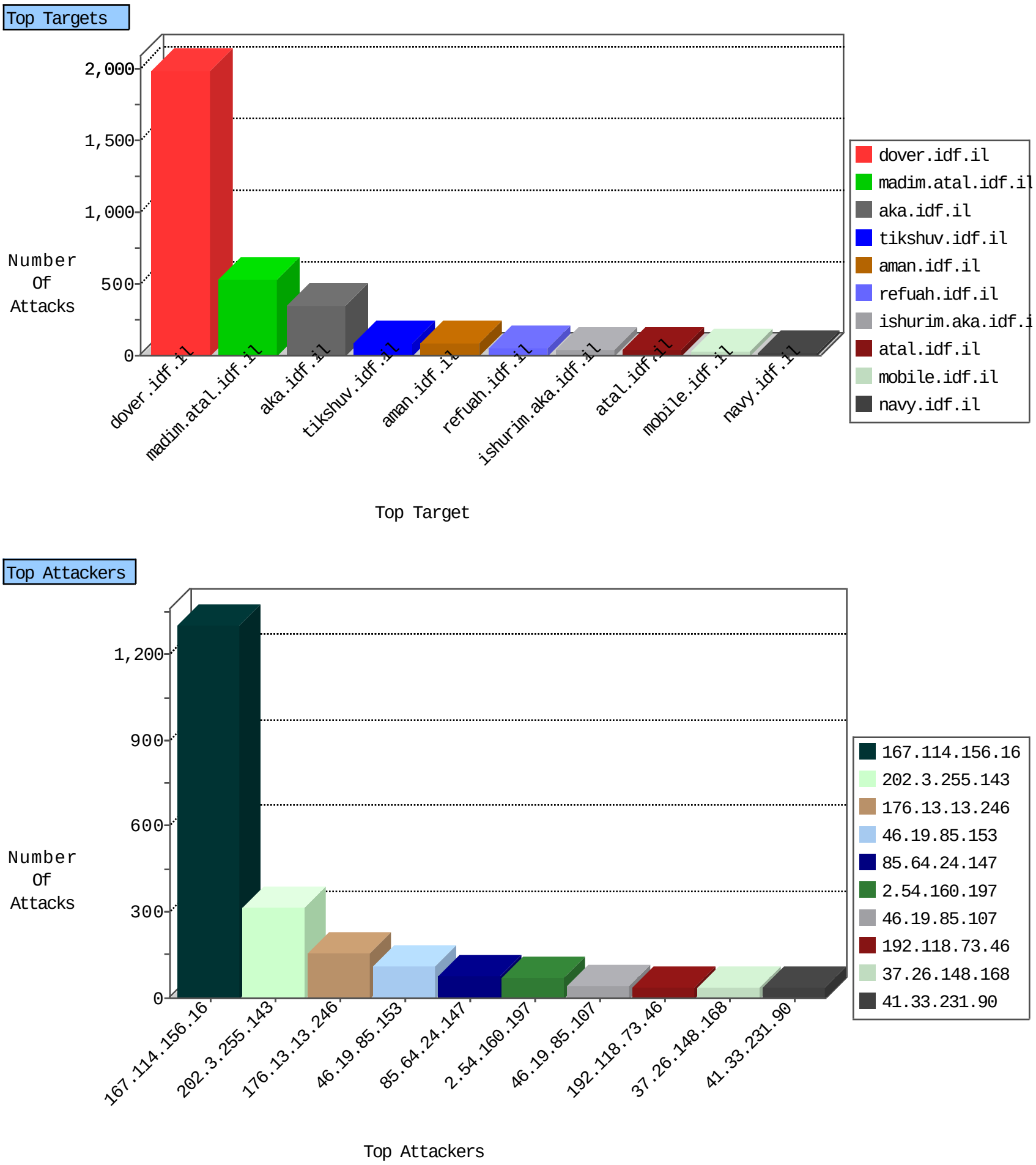
01-17-2016-17:04:06 to 01-17-2016-18:04:06

IDF Under Attack
Daily Report



01-17-2016-17:04:06 to 01-17-2016-18:04:06

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	3005
141.212.122.199	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
188.138.17.205	France	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

01-17-2016-17:04:06 to 01-17-2016-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-17-2016-17:04:06 to 01-17-2016-18:04:06

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	276
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.183.25.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.254.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.75.110	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.75.110	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -f -sS	1
187.105.83.64	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.198.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.8.132.78	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.149.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.245.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.132.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.22.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.13.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.152.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.75.110	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
37.26.146.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.92.221.171	147.237.72.166		aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
2.52.14.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.127.0.45	147.237.76.202	Italy	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
109.66.54.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.1.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-17-2016-17:04:06 to 01-17-2016-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
192.118.73.46	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
185.120.125.6		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.154.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.67	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.120.126.78		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
205.197.242.145	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
24.44.84.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
109.64.209.74	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.142.243.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
2.52.46.55	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.35.92	Israel	147.237.72.166	aka.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
5.22.135.136	Israel	147.237.72.166	aka.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	alert	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.35.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.76.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.38	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.118.73.46	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
103.29.249.252	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.181.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	drop		drop	6
79.181.183.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.148.241	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.73	Israel	147.237.72.166	aka.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

01-17-2016-17:04:06 to 01-17-2016-18:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.13.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
85.64.24.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
2.54.160.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
176.13.13.246	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.13.246	Block	52
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
85.250.188.173	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.206.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.54.40.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
2.54.19.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.27.105.94	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 185.27.105.94	Block	5
5.22.135.136	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.22.135.136	Block	5
31.173.101.118	Romania	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
109.253.141.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.40.26	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.158.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.160.191.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.54.181.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.55.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
96.30.10.64	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.214.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.212.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
69.64.33.234	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
110.77.211.15	Thailand	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
96.30.10.64	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
46.19.85.130	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation txtContent in www.tikshuv.idf.il/modules/forums.frm/frmmessage.aspx	Block	2
2.52.158.67	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	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
46.120.235.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
46.121.136.144	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.99.98.54	Canada	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.9.60.113	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
79.178.207.87	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
173.252.74.101	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.107.38	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
142.4.7.164	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
211.1.231.194	Japan	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
89.163.146.245	Germany	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
187.45.195.63	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
69.195.124.103	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
198.57.162.202	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
41.76.106.243	South Africa	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
84.228.153.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.122.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-17-2016-17:04:06 to 01-17-2016-18:04:06