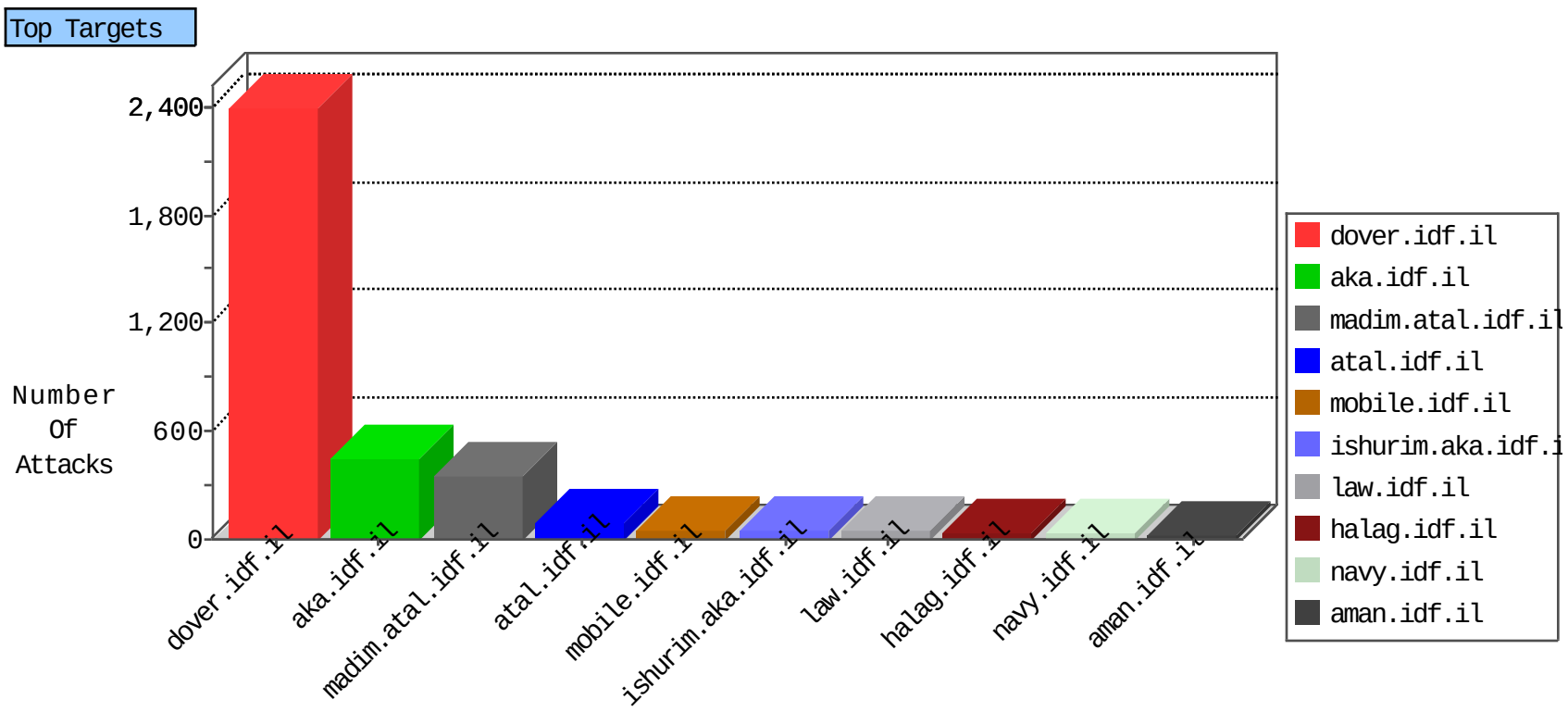
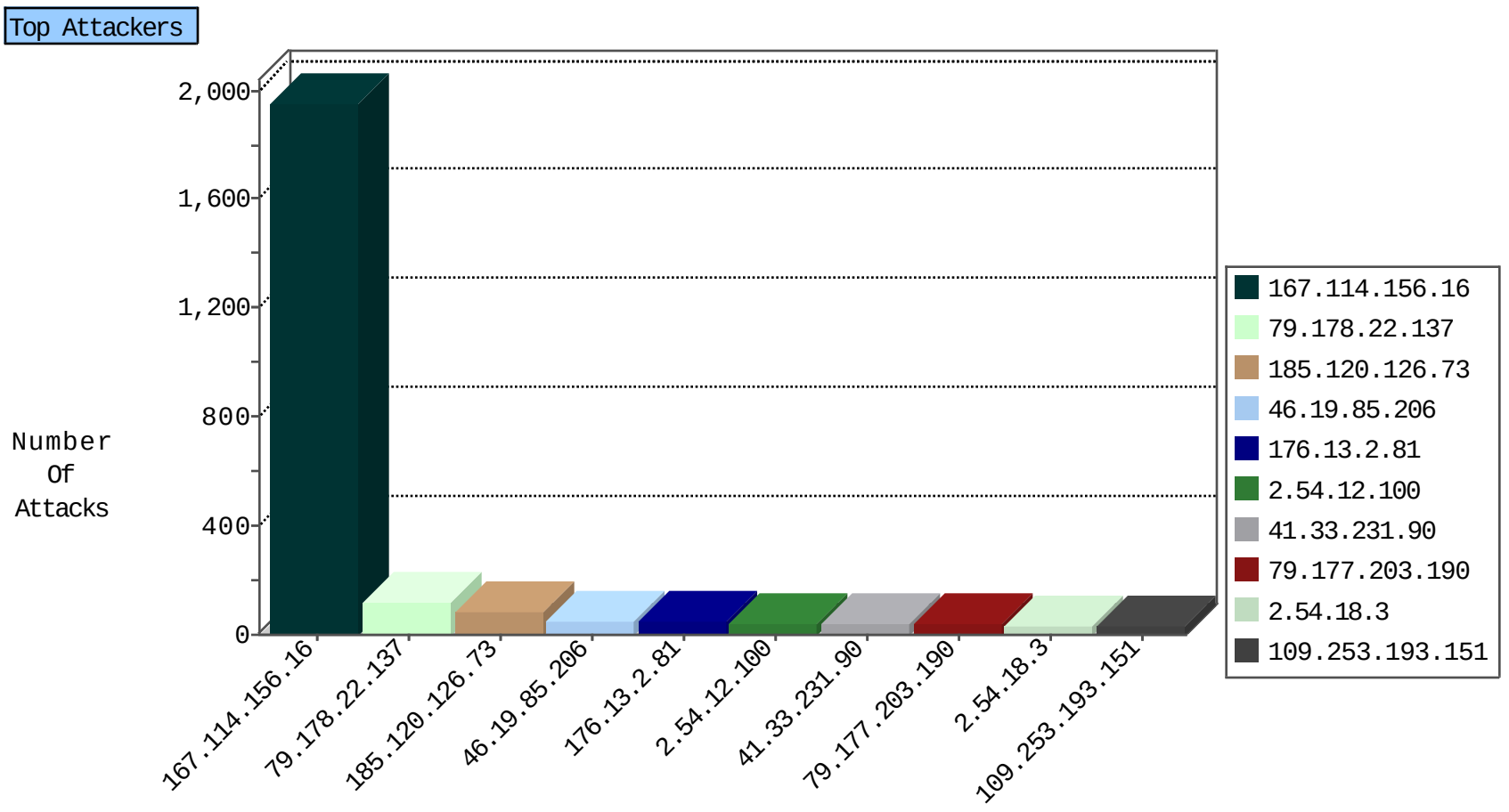
01-05-2016-15:04:03 to 01-05-2016-16:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-05-2016-15:04:03 to 01-05-2016-16:04:03

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	3359
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	632
85.64.128.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
59.168.120.146	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
37.59.155.60	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.56	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
88.247.117.156	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-15:04:03 to 01-05-2016-16:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-05-2016-15:04:03 to 01-05-2016-16:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.206	147.237.77.233	Israel	atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
108.163.222.38	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.117.13.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.49.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.168.27.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.48.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.95.84.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.126.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.3.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.132.100.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.72.167	Turkey	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.115.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.161.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.40.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.202.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.195.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-05-2016-15:04:03 to 01-05-2016-16:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
2.54.12.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
46.19.85.206	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	22
31.154.173.51	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
84.95.134.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
80.179.102.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
80.246.136.200	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	12
107.167.112.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.77	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
172.56.26.254	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
213.57.235.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
78.188.138.25	Turkey	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.64.128.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.136.200	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.228.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.114.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.91.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.77	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.180.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.57.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.178.22.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.35.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.117.125.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.111.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.231.192.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.166.114.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
78.188.138.25	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.23.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
187.45.193.215	Brazil	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
213.57.235.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.249.120.166	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.26.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.128.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
213.57.235.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.147.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.181.228.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.57.235.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.136.200	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.235.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

01-05-2016-15:04:03 to 01-05-2016-16:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.22.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
176.13.2.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
79.178.22.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.22.137	Block	41
109.253.193.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.18.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.221.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.147.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.54.34.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
212.179.21.194	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.54.183.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
108.163.222.38	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 108.163.222.38	Block	7
2.54.12.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.211.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
78.188.138.25	Turkey	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	4
212.76.97.68	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.76.97.68	Block	3
2.54.182.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.143.169.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
80.246.136.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.235.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.156.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.23.38	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	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
176.13.23.38	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	2
212.76.97.68	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/&sa=u&ved=0ahukewj8mofj55lkahwds3ikhwrcci4qfggnmaa&usg=afqjcnhdhx85tdz_a0-eyy7o0ff9_7steg	Block	2
84.111.128.97	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
81.218.104.109	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	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
5.22.129.70	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.26.147.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.18.3	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** *******, Observed ********** ********** ********** *	None	2
192.116.215.34	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	2
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspxâ€?â€Ž	Block	2
109.160.165.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.126.40.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.162.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
5.28.157.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.95.134.68	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
50.62.177.153	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
164.215.110.7	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/javascript:	Block	1
80.179.5.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.114.146.227	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.152.22	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.128.148.119	Netherlands	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1

01-05-2016-15:04:03 to 01-05-2016-16:04:03