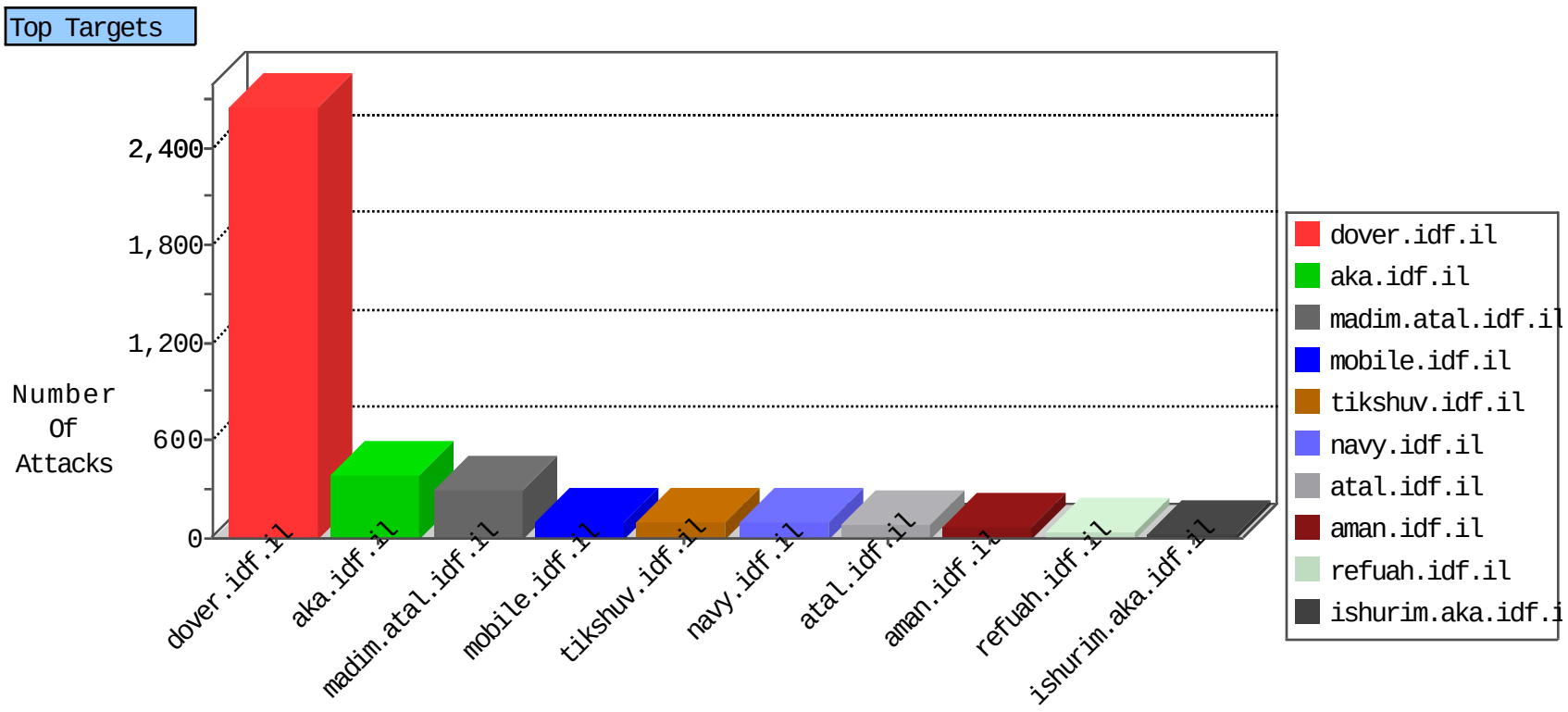
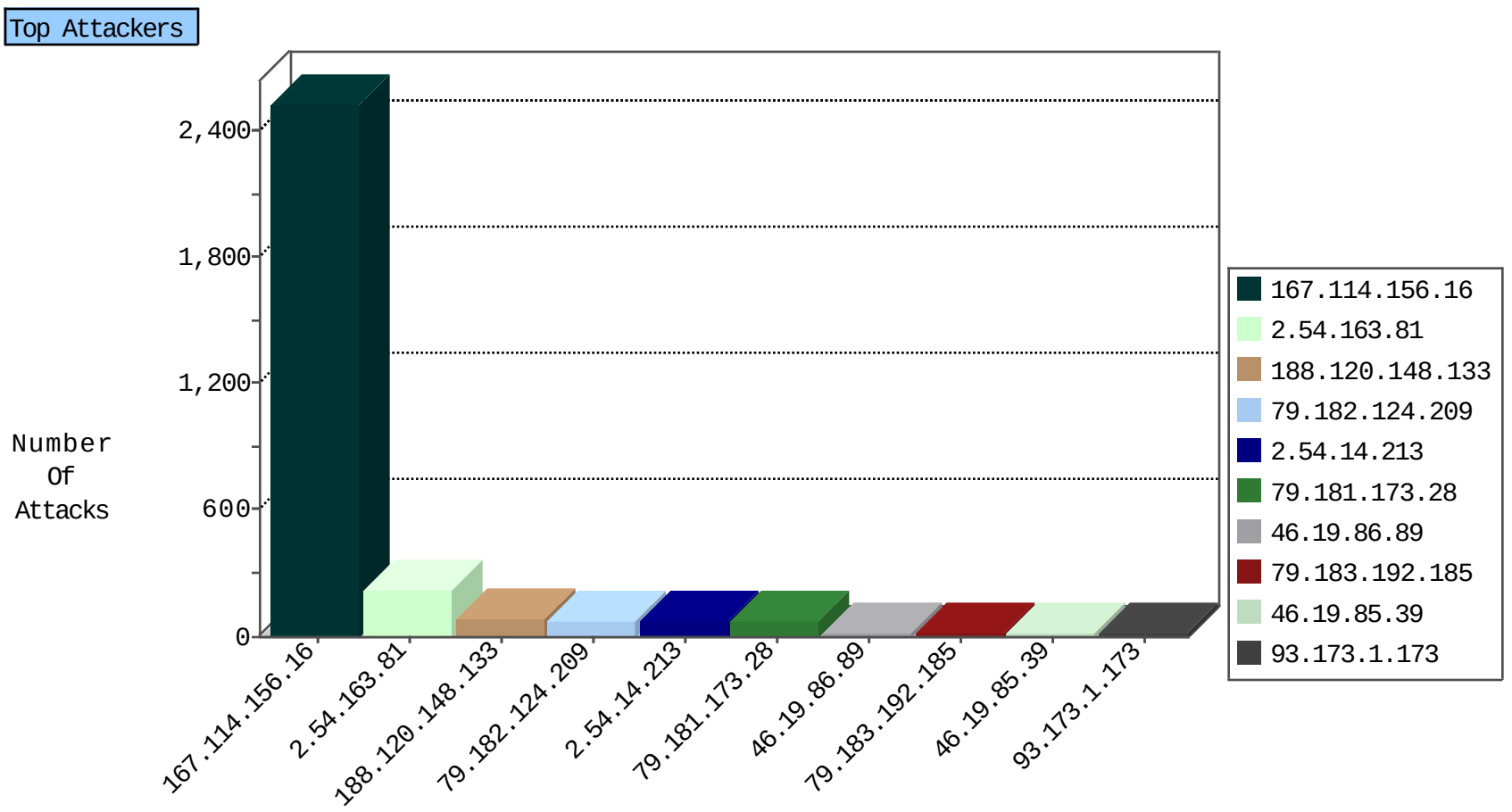
03-13-2016-17:04:00 to 03-13-2016-18:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-13-2016-17:04:00 to 03-13-2016-18:04:00

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	3596
79.183.231.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
123.151.42.61	China	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1

03-13-2016-17:04:00 to 03-13-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.192.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
93.173.1.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
138.134.102.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.108.204.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.88.118.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.109.13.58	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.78.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.139.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
82.80.55.126	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-13-2016-17:04:00 to 03-13-2016-18:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.120.148.133	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	89
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.179.27.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
113.59.33.61	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1
40.121.136.51	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
109.65.113.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.215.89.20	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
88.249.106.23	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.120	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
80.246.138.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.60.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.190	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.134.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.198.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.61.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.215.89.20	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.137.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.168.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.174.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.56.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-13-2016-17:04:00 to 03-13-2016-18:04:00

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	SYN Attack	SYN -> SYN-ACK -> RST	reject	82
79.181.173.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
2.54.163.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	27
46.19.86.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
194.90.209.235	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
79.183.32.150	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
5.29.116.155	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.160.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.40.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
156.205.72.163		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.149.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.124.209	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.203.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.30.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.49.191	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.19.72	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
2.54.188.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.30.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.23.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.34.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.48.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.134.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.40.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
80.246.139.189	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		alert	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	4
79.178.136.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.67.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.188.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.164.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.212.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.143.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.144.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.15	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.161.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.86.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-13-2016-17:04:00 to 03-13-2016-18:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.80.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.137.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-13-2016-17:04:00 to 03-13-2016-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.163.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	178
2.54.14.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.15.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.132.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.65.212.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.182.146.186	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
79.182.146.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	4
80.178.157.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.137.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.90.131.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.29.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.210.106	Block	3
192.117.138.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
174.129.237.157	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
131.253.25.225	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.217	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	2
46.19.85.12	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
176.13.1.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
62.219.34.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	1
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.148.219	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.80.195	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	1
183.206.175.39	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 183.206.175.39	Block	1
140.115.111.116	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/favicon.ico	Block	1
46.120.31.194	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.120.31.194	Block	1
87.70.31.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.182.120.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.14.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
80.246.137.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.178.189.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
183.206.175.39	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/scripts/fckeditor/editor/	Block	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
54.205.196.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
108.7.54.151	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
46.19.85.196	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.188.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.124.209	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2969.jpg	Block	1
46.19.86.168	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
131.253.25.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.81.23.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17899-he/dover.aspx„'¦'ƒ„'¬„¯„ƒλ€Š„'¿„ƒ„'½„'š€λƒ„'¬„¯„ƒλ€Š„'¿„ƒ„'½„'š€λƒ„'¬„¯„ƒλ€Š„'¿„ƒ'½„'š€λ•	Block	1
79.180.124.1	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-13-2016-17:04:00 to 03-13-2016-18:04:00