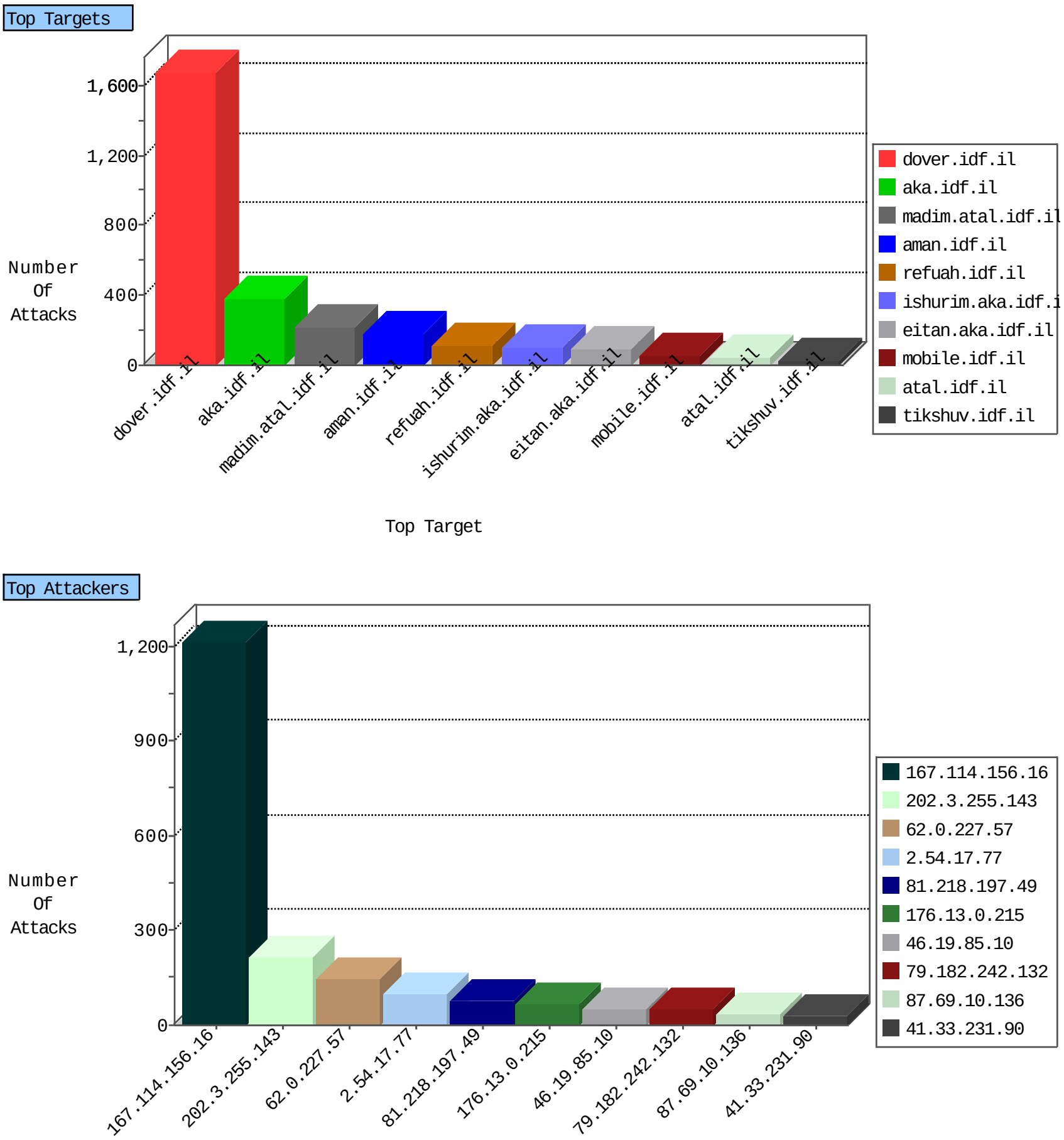
01-17-2016-15:04:06 to 01-17-2016-16:04:06

IDF Under Attack Daily Report



01-17-2016-15:04:06 to 01-17-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4858
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3333
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2150
212.25.121.195	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
79.176.4.161	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
27.55.97.10	Thailand	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
109.163.234.7	Romania	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
84.106.158.108	Netherlands	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
72.131.9.235	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
93.190.152.161	Europe	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
72.131.9.235	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
104.236.107.249		147.237.0.16	my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1

01-17-2016-15:04:06 to 01-17-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-17-2016-15:04:06 to 01-17-2016-16:04:06

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	183
94.230.86.224	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	12
80.246.133.220	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
54.147.176.220	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
171.112.96.169	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
37.26.146.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
171.112.96.169	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.52.189.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.66.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.145.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.101.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.223.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.48.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
171.112.96.169	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
171.112.96.169	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.44.139.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
171.112.96.169	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
111.85.219.12	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
109.64.157.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.148.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.109.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.167	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-17-2016-15:04:06 to 01-17-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.227.57	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	147
81.218.197.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.19.85.10	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
79.182.242.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
107.167.107.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
87.69.10.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
212.199.57.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
80.246.133.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.120.126.74		147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.253.218.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.194.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
62.219.191.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.228.132.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
90.184.141.245	Denmark	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.114.91.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.117.148.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.239	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.10.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
83.130.107.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.126.196.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.159.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.141	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.177.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
199.203.122.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
112.78.4.244	Vietnam	147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
217.174.148.119	Bulgaria	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
176.31.229.182	France	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.133.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
193.232.92.8	Russian Federation	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.128.142.89	Poland	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.66.199.49	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.167.190.179	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.199.57.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.168.207.28	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
187.17.98.219	Brazil	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.150.66.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.17.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
176.13.0.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
176.13.4.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	13
176.13.5.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.20.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.133.172	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	4
212.143.158.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	4
109.253.218.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
162.144.222.195	United States	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/	None	2
49.197.14.209	Australia	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.221.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
198.15.125.34	United States	147.237.72.166	aka.idf.il	Unknown Parameter author in aka.idf.il/	None	2
176.13.13.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.251.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
212.116.187.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
106.186.21.169	Japan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
10.162.80.6		147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	2
84.228.236.183	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	2
106.186.21.169	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/libraries/jmail.php	Block	2
173.252.88.91	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.63.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.56.96	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
54.243.53.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12386-en/dover.aspx	Block	1
80.246.139.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.117.147.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.176.155.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.11	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
173.252.112.98	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
27.50.89.230	Australia	147.237.76.147	chinuch.aka.idf.il	Unknown Parameter author in www.chinuch.aka.idf.il/	None	1
89.139.238.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
216.72.40.185	Israel	147.237.72.156	aman.idf.il	Multiple Or a=a SQL Injection trial(+) from 216.72.40.185	Block	1
2.54.18.86	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
84.110.111.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
159.203.120.25	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
109.253.194.6	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.183.185.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.146.144.195	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1