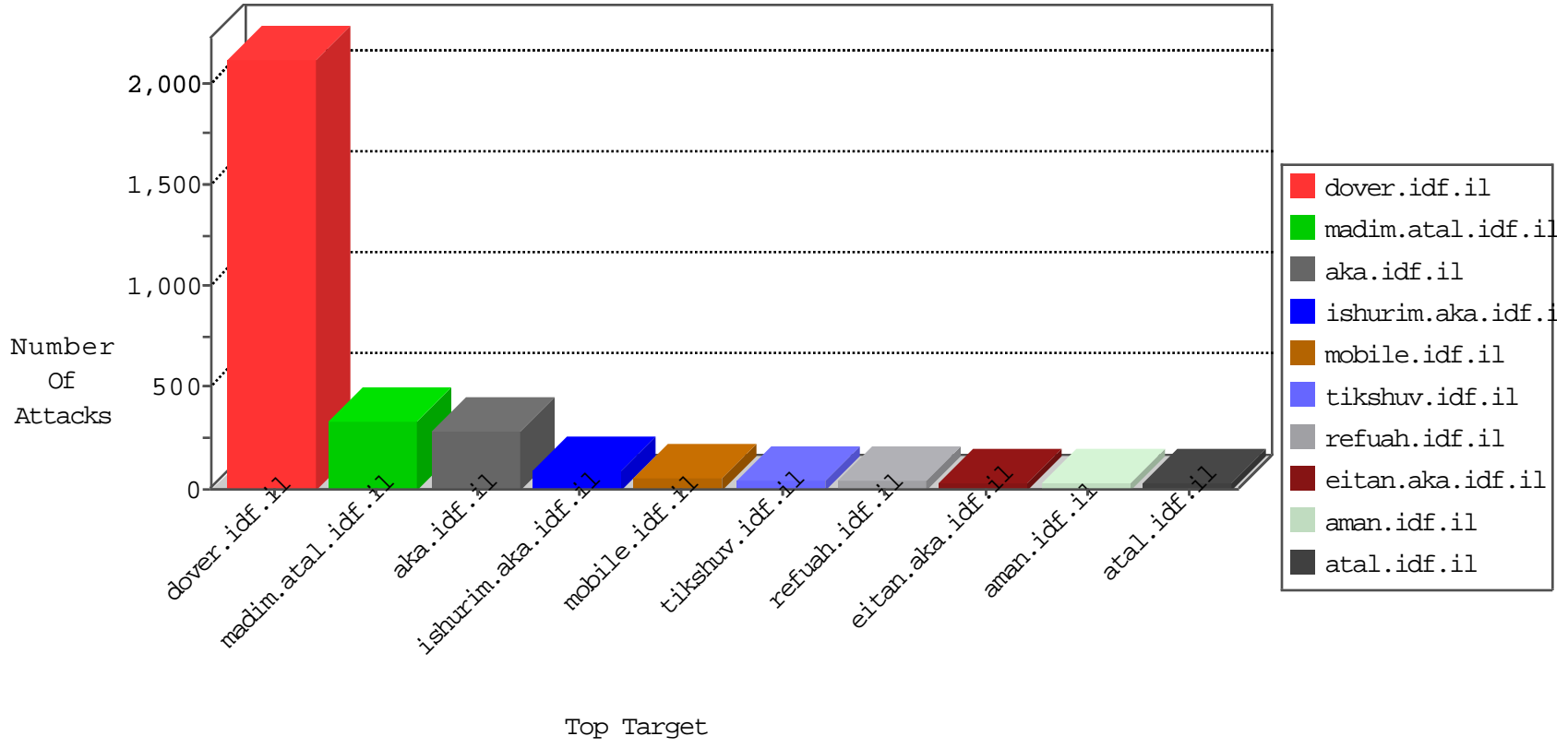


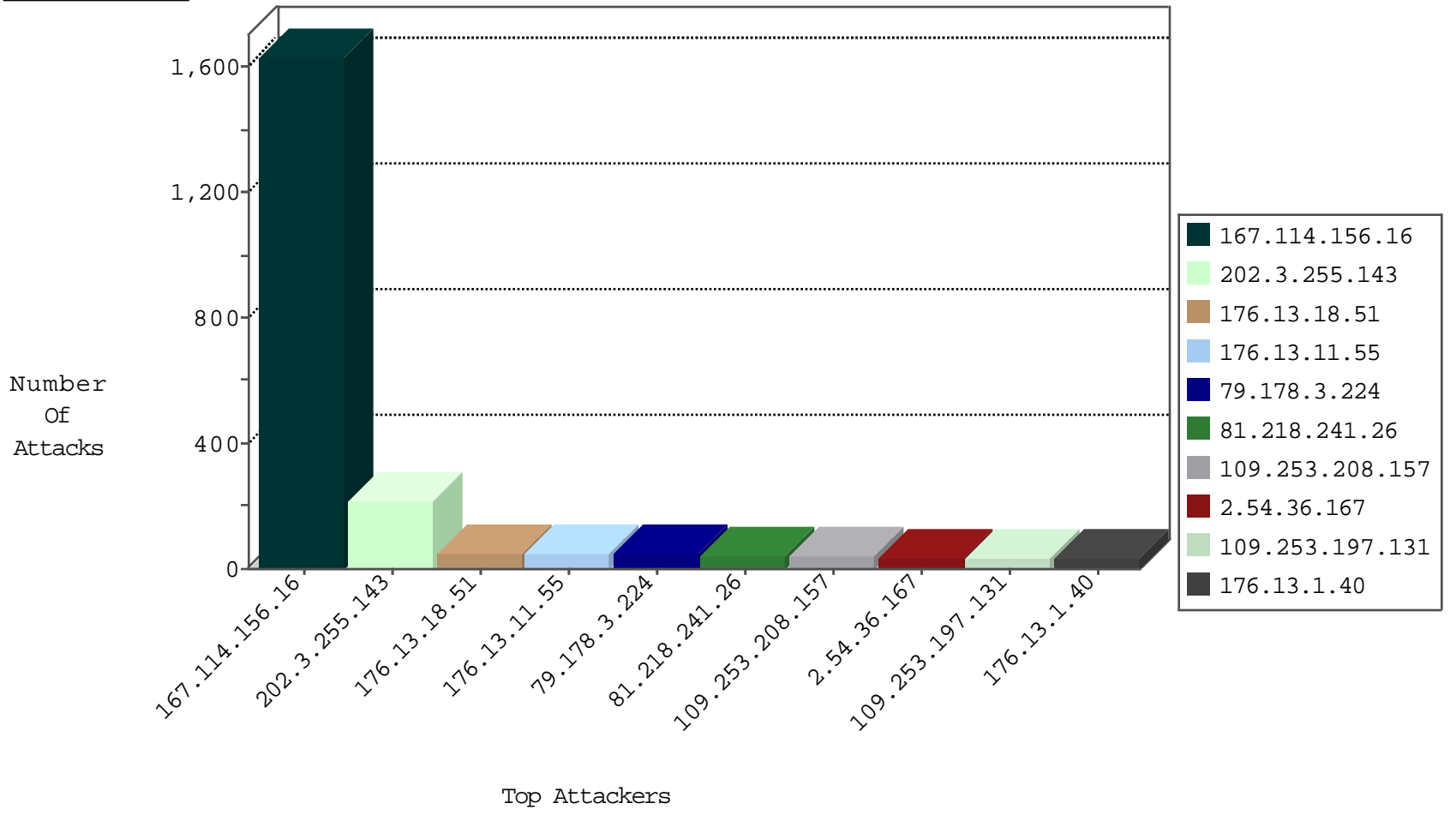
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3208
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
79.177.11.229	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
113.64.47.110	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
89.248.172.159	Netherlands	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Top	drop	2
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-18-2016-09:04:00 to 01-18-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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	179
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.253.203.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.54	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.236.74.6	147.237.76.200	Poland	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.231.193.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.181.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.46.1.66	147.237.77.216	Thailand	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.49.54	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
94.102.49.54	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.236.74.6	147.237.0.19	Poland	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.159	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.79.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

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	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.193.135.230	France	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	27
79.178.3.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
138.134.102.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
2.54.36.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
107.167.108.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
79.178.3.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.32	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
79.177.208.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.152.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.148.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.56.62	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.106.46.74	Palestinian Territory Occupied	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.138.60	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
80.246.139.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.167	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.27.53	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.234	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.139.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.50	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.128.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.41.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.163.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.172	Israel	147.237.77.243	mobile.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
46.19.85.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.173.7.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
87.69.230.66	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.20.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
213.57.158.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.11.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
109.253.208.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.197.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
176.13.1.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.13.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.192.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.149.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
109.253.136.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
217.194.202.179	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 217.194.202.179	Block	15
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
62.219.187.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/	Block	4
2.54.155.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
62.219.187.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sip_storage/files/4/	Block	3
2.54.24.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.13.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/homas/site/	Block	2
173.252.80.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 46.211.34.236	Block	2
93.172.142.54	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	2
173.252.80.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	2
176.13.22.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.244.96	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.52.24.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.75.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589- en/dover.aspx	Block	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
46.211.34.236	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Admin Blocking from 46.211.34.236	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
2.54.152.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.89.231	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.82.64.68	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to qassam.ps/files/martyrs/37ee9280da.jpg	Block	1
213.57.158.224	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1093-7972-he/eitan.aspx	None	1
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.5.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.23.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
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	1
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 81.218.241.26	Block	1
80.178.157.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.230	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.158.224	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1