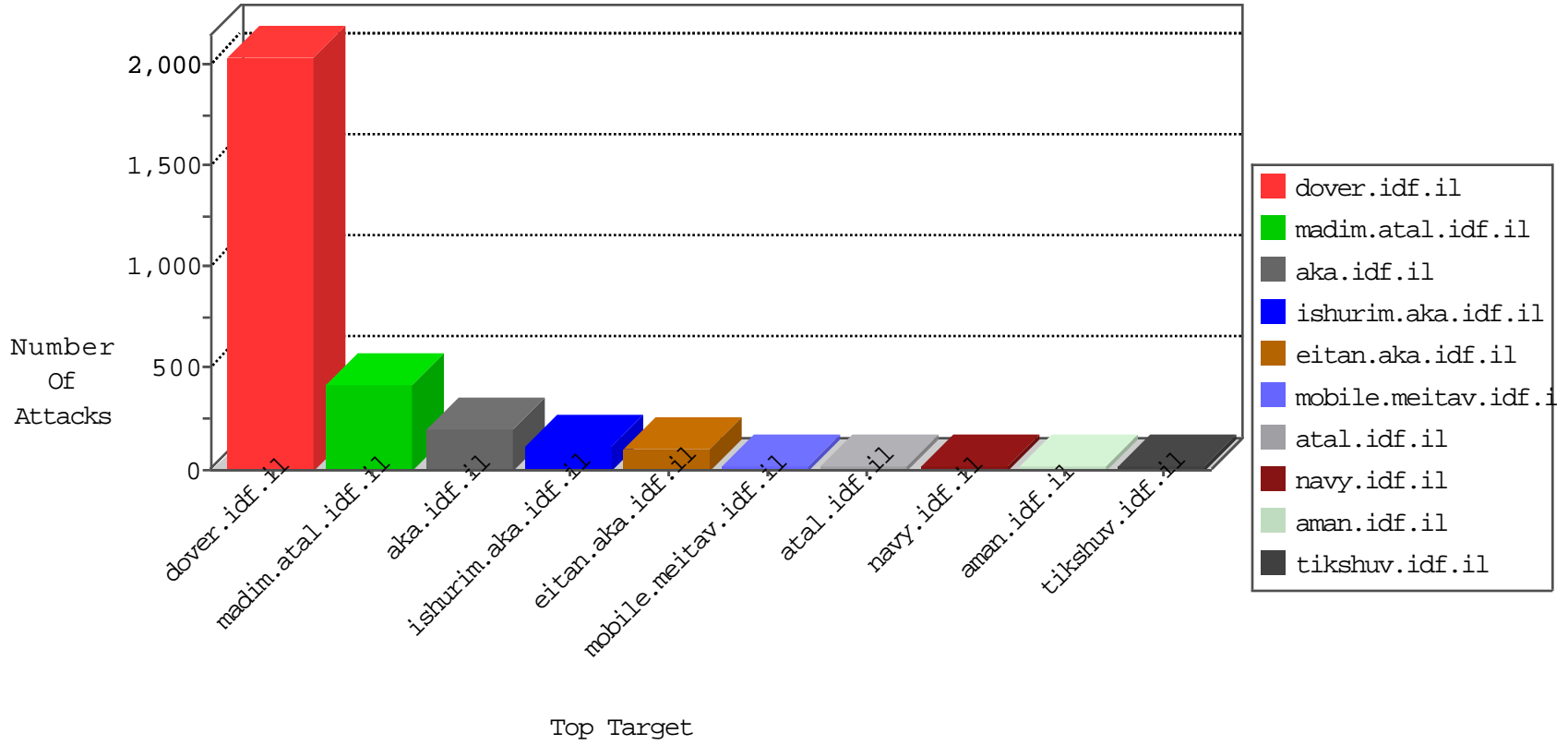




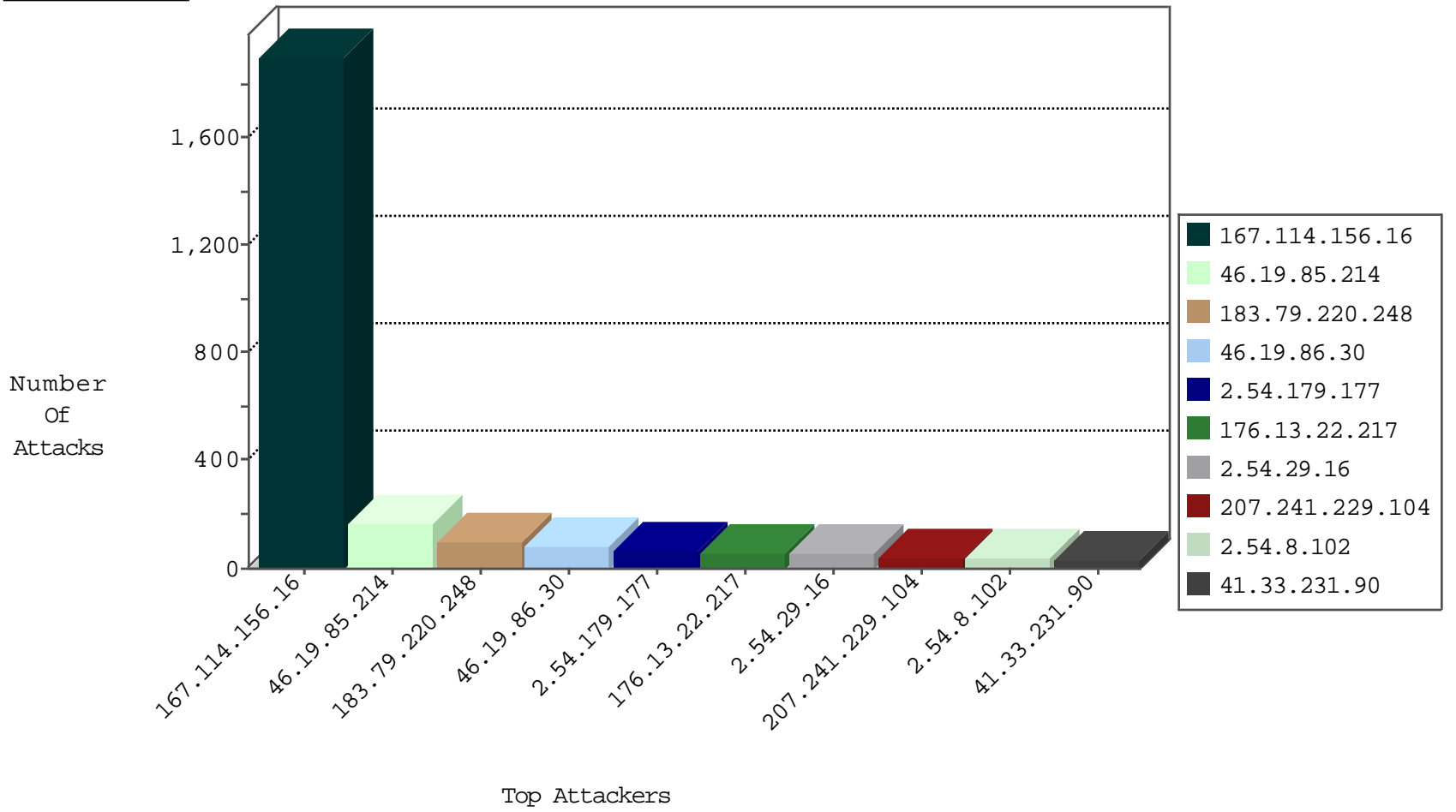
IDF Under Attack Daily Report



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	3169
208.100.26.228	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
5.189.176.176	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
5.189.176.176	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
5.189.176.176	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
5.189.176.176	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
114.226.158.195	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
5.189.176.176	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

12-17-2015-08:04:04 to 12-17-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.8.102	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
46.19.85.42	147.237.76.39	Israel	mobile.meitav.idf.i	POLICY-OTHER TCP packet with urgent flag attempt	16
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
207.241.229.104	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
164.138.118.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.182.195.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.177.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.14.65	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
185.32.179.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.90.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.107	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.30	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	83
207.241.229.104	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
2.54.179.177	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.8.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
183.79.220.248	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	16
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.190	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.0	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.219.166.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
183.79.220.248	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
84.228.138.173	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
130.207.203.56	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
37.26.149.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.212.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.212.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.74.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.196.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.57.61	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.173	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.81	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
2.52.40.246	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
85.250.215.80	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.199.149	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.54	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.40.246	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.42	Israel	147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	3
85.65.169.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
80.178.169.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.54	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.40.246	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.191.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.203.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.238.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.20.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.40.246	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.140.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.71.145.156	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.52.173.219	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.120.148.209	Israel	147.237.76.30	hinush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.137.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.40.246	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.181.168.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
2.54.29.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
176.13.22.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.179.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
183.79.220.248	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.220.248	Block	39
183.79.220.248	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.220.248	Block	39
176.12.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	7
2.54.131.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.143.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	3
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	3
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.8.204.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.46.35.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.36.140	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
185.32.179.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
46.116.153.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
109.253.196.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.16.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.127	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.127	Block	1
2.52.141.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.16.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.115.84	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
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	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.30.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.58.178.58	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
176.13.10.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.221.243	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.202.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.149.58	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
207.46.13.127	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	1
2.54.0.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.115.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.75.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	1
212.143.82.238	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.125.14.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct125 in www.aka.idf.il/main/sachar/payslips.aspx	None	1