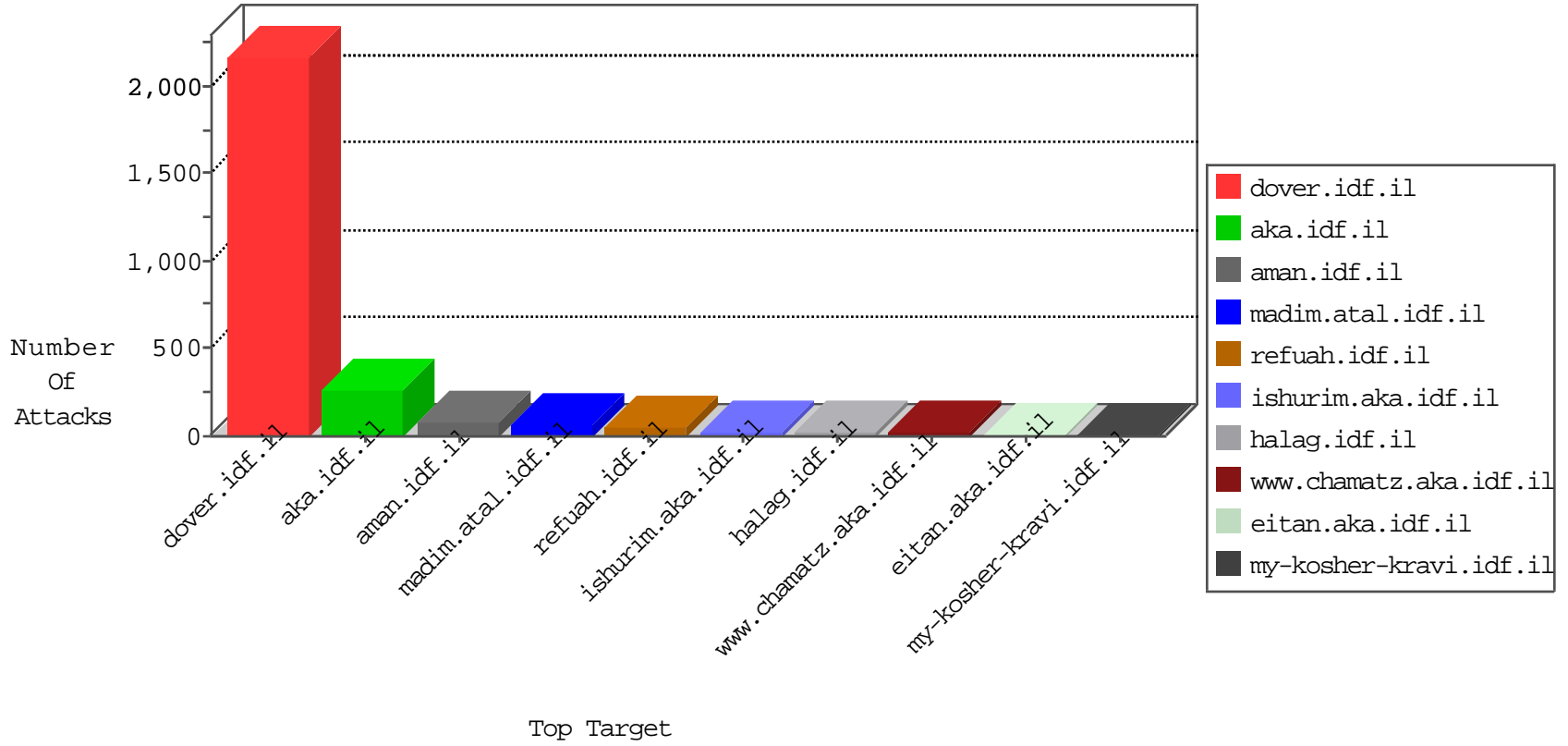


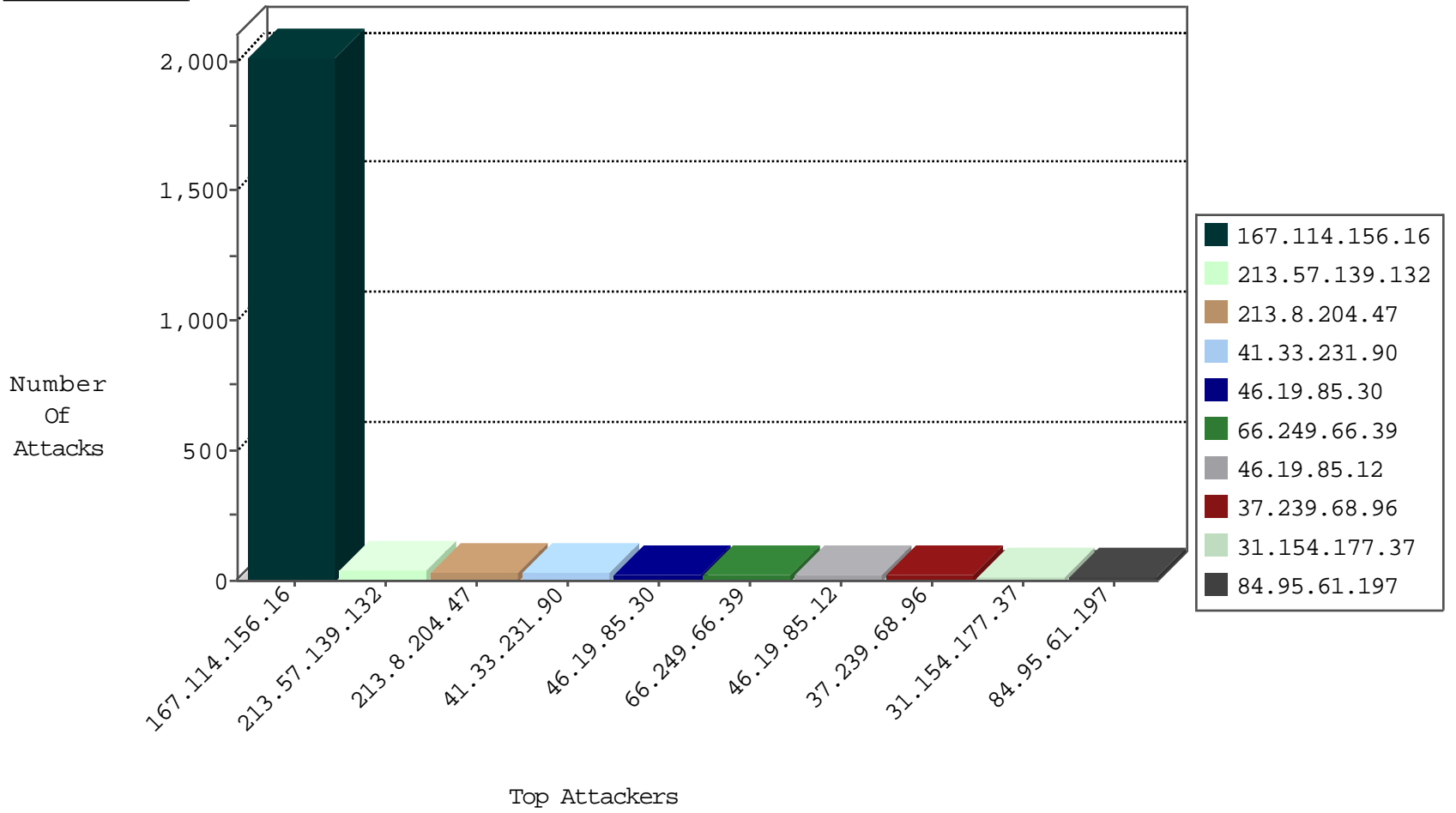
IDF Under Attack Daily Report



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	3328
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
89.248.160.229	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.34	ychalan.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.229	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
118.193.21.98	China	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
67.79.13.53	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.229	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.229	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.93.90.96	France	147.237.72.166	aka.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.26	France	147.237.72.166	aka.idf.i	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
54.67.48.51	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.129	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
54.67.48.51	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.67.48.51	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.108.132.58	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
54.67.48.51	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.67.48.51	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
54.67.48.51	147.237.72.217	United States	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
107.10.41.73	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
54.67.48.51	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.67.48.51	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.67.48.51	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.147.86.4	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.67.48.51	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
213.57.139.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
213.57.139.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.95.61.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
109.64.98.32	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.89.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.132.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.154.177.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
31.154.177.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.144.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.65.211.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.206.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.210.179.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.131.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.239.68.96	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.130.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.48.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.239.68.96	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.5.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.144.17	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.154.150.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
82.80.193.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.154.150.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.3.146.146	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.40.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.5.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.130.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.154.150.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.143	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
31.210.186.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.170.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.38.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.151.118	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.186.42.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.227.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.211.105	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.212.121.192	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
77.125.97.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.229.30.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.157.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.135.68	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
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.13.2.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.133.34	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	4
149.78.250.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
2.54.15.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
177.12.172.102	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 177.12.172.102	Block	4
2.52.15.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	3
2.52.182.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.13.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.142.55	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation returnUrl in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	2
91.192.111.247	Spain	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.20.218.249	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
85.65.96.71	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
80.246.139.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.173	Block	2
79.180.138.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	2
46.121.25.44	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	1
176.12.143.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.143.55	None	1
85.64.224.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.183.144.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter @ID in www.aka.idf.il/gyus/general/	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.108.132.167	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
79.178.131.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.70	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
91.192.111.247	Spain	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
178.154.243.93	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
109.201.152.22	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
81.218.135.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.141.34	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
107.150.56.90	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
79.180.178.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.47	Israel	147.237.72.156	aman.idf.il	XSS - Basic 3	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.86.82.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.28.165	Israel	147.237.76.42	refuah.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 85.65.28.165	Block	1
176.12.148.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
45.36.3.35		147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/portalmilum/templates/home.asp	Block	1
109.65.211.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.26.147.228	Block	1
95.108.132.184	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
79.179.131.206	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	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1