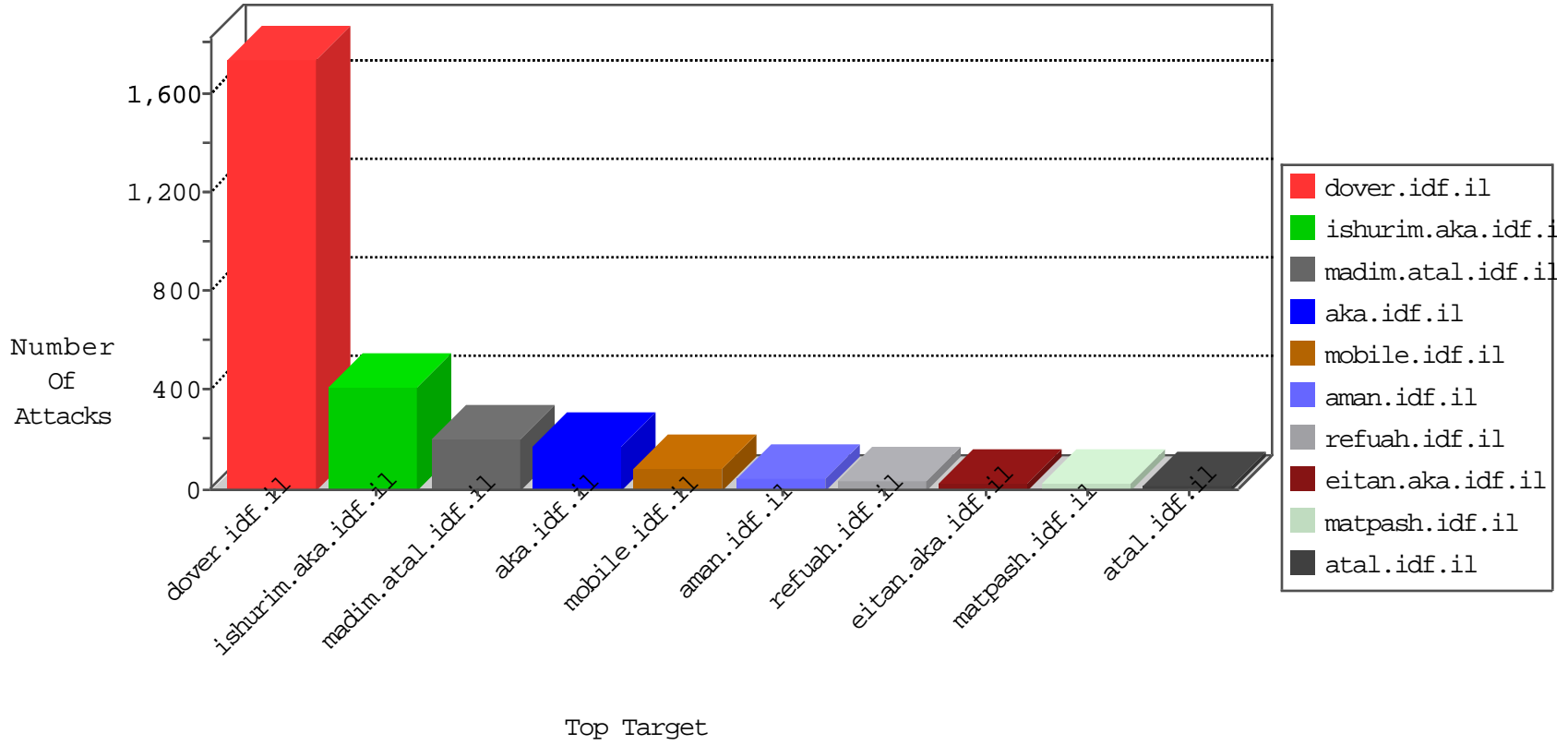


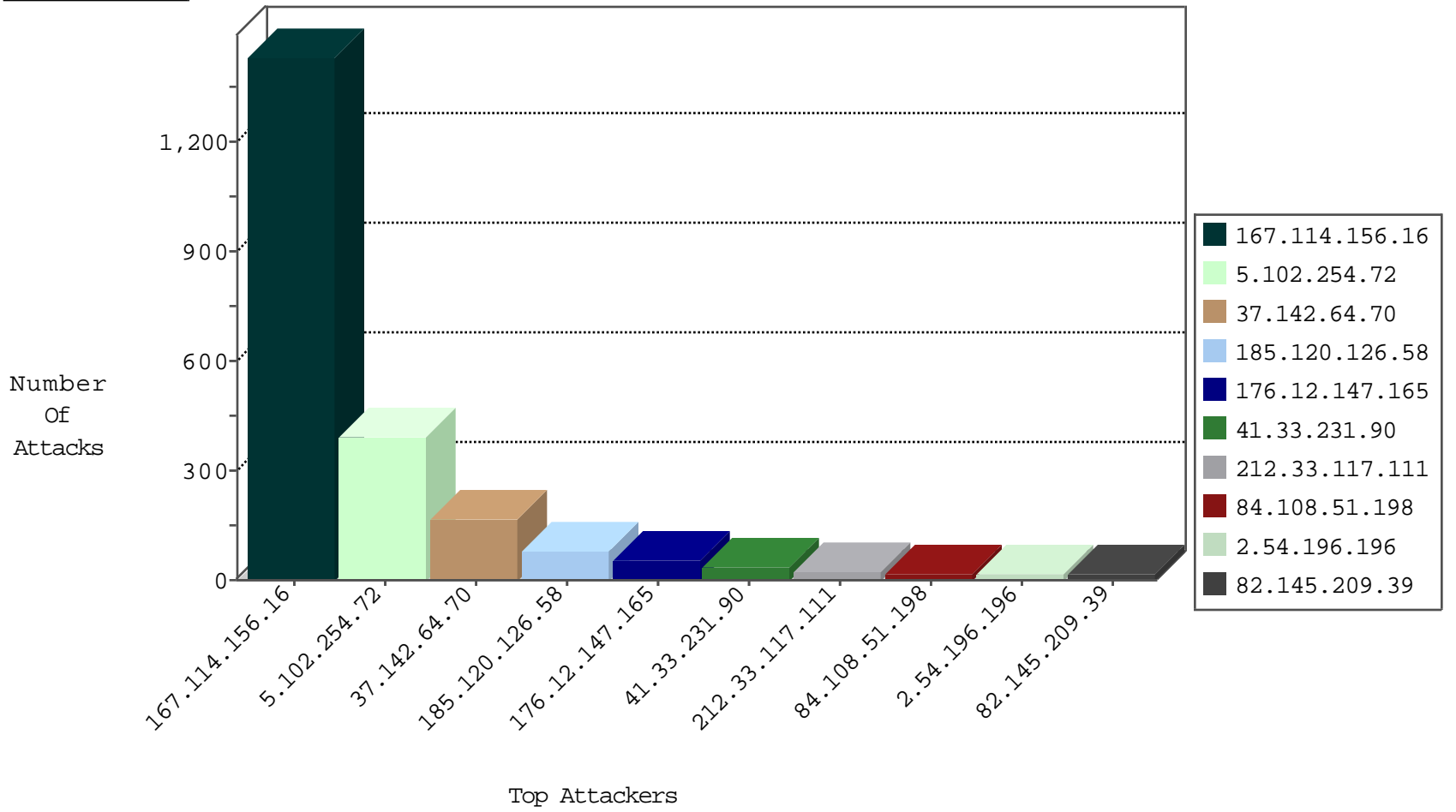
IDF Under Attack Daily Report



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	3127
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	957
82.145.209.39	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
115.231.222.40	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
46.166.139.20	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-13-2015-22:04:04 to 12-13-2015-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
136.243.110.172	Germany	147.237.77.234	halag.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	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
177.19.158.160	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN NMAP -f -sS	1
112.33.8.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
112.33.8.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
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	1
99.39.117.129	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
189.194.44.49	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.250.93.199	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
187.161.113.16	147.237.77.235	Mexico	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.250.93.199	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
187.161.113.16	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.19.158.160	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
112.210.208.29	147.237.76.38	Philippines	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.33.8.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.155.65.247	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
91.218.246.103	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.103.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.194.44.49	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.250.93.199	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1
187.161.113.16	147.237.77.216	Mexico	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.250.93.199	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
177.19.158.160	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.254.72	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	390
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.12.147.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
185.27.105.167	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.33.117.111	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.197	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.20.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.172.180	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.64.70	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
141.0.14.146	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.196.196	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.67.171.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.229.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.51.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.33.117.111	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.253.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.5.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.140	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.121.78.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.196.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.186.147.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.51.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.196.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.51.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
67.8.231.215	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.51.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
40.77.167.59	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.122.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.7.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.164.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.8		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.233.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.112.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.48.34.102	Czech Republic	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
37.142.64.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.142.64.70	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.64.70	Block	68
176.12.147.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
2.52.45.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.12.147.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	6
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.250.186.42	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
79.183.229.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.173.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.131	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
176.12.139.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.65.149.119	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
37.142.64.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.243.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.218	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
176.13.1.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.216.206	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/1133-22638-he/dover.aspx.	Block	1
84.108.49.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
54.153.33.145	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
37.142.193.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.29.107.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.119	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
141.212.122.97	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.117.153.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.177.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.109.16.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.152.234.175	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.52.140.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.12.147.165	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.147.165	Block	1
77.125.138.22	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
109.66.29.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar/tfasim.aspx	Block	1
62.90.215.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.85.5	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
95.86.113.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewiq-7tx0tnjahvcubokhci zcm8qfggxmai&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
80.246.136.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.119	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.15.119	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
149.78.76.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
109.64.15.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.133.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1