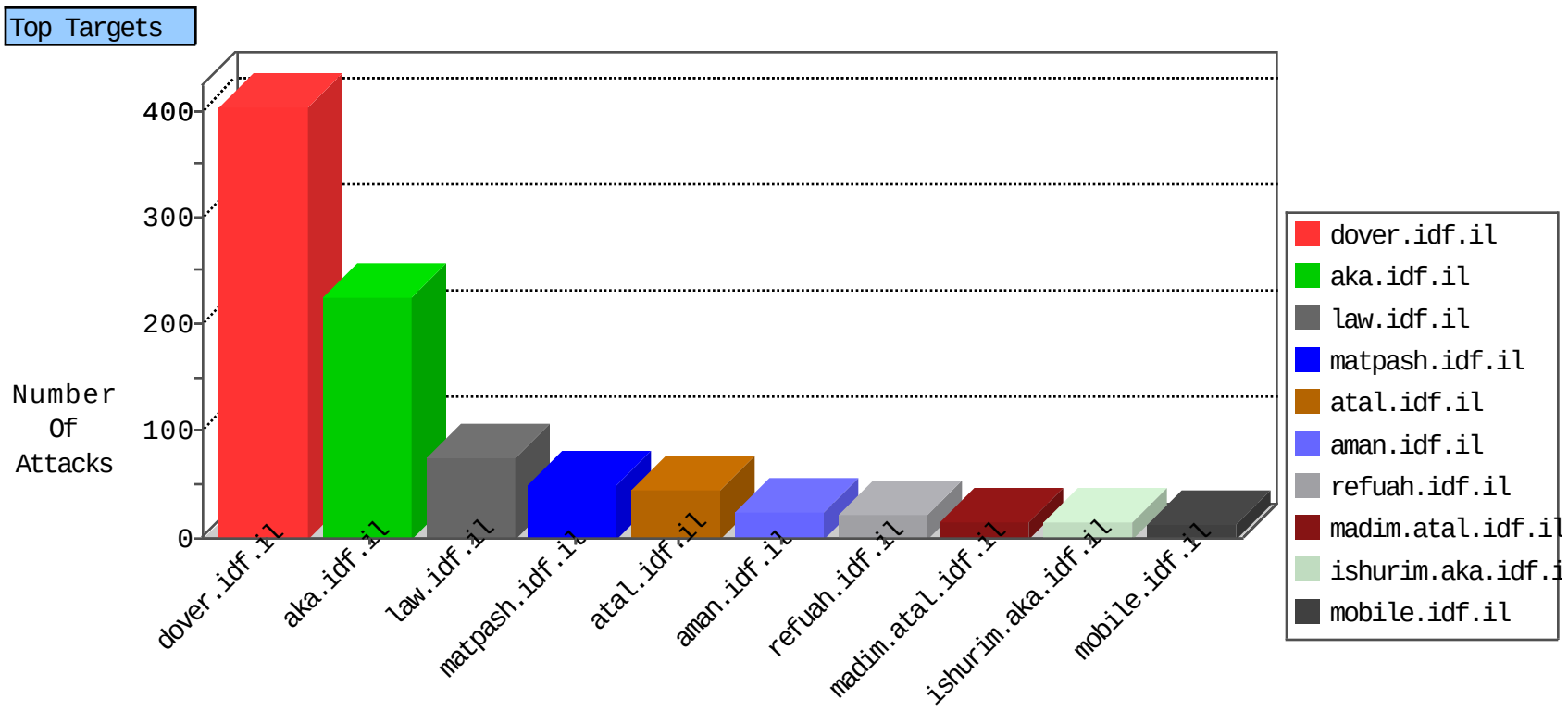
04-26-2016-00:04:03 to 04-26-2016-01:04:03

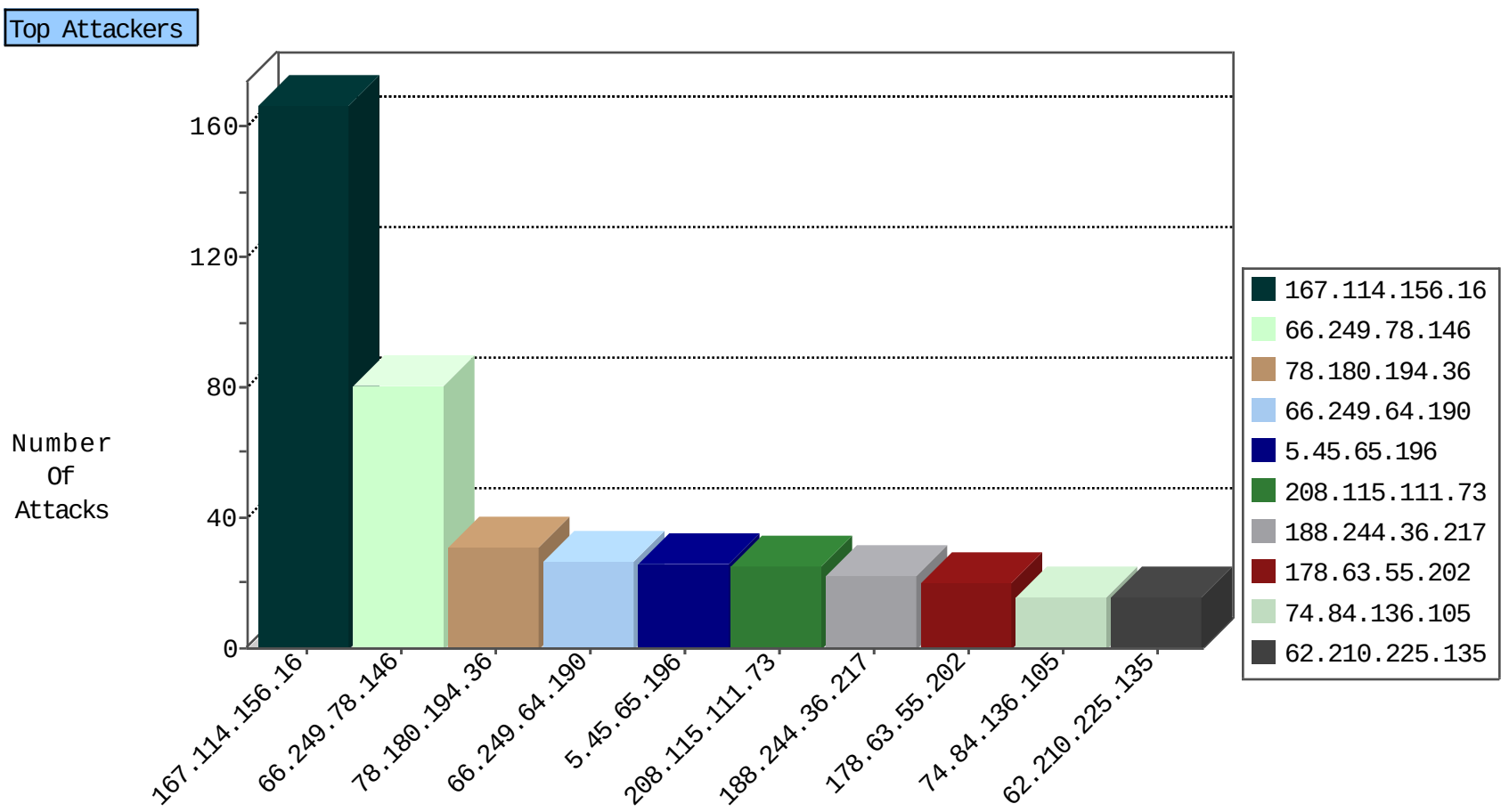
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-26-2016-00:04:03 to 04-26-2016-01:04:03

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	HTTP-POST-Segmented-DoS	dest-reset	7795
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1176
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.223.201.10	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
45.63.20.231	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
52.28.32.164	Germany	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Https	drop	1

04-26-2016-00:04:03 to 04-26-2016-01:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.45.65.196	Netherlands	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.84.136.105	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.45.65.196	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-26-2016-00:04:03 to 04-26-2016-01:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.45.65.196	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	14
74.84.136.105	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	12
108.67.169.124	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
117.20.41.62	147.237.77.227	Singapore	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.253.150.80	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.160.160.49	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
209.126.230.74	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
78.180.194.36	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
200.195.135.82	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
109.253.136.153	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
200.195.135.82	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
78.180.194.36	147.237.77.176	Turkey	matpash.idf.il	SERVER-WEBAPP admin.php access	1
200.195.135.82	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -f -sS	1
66.223.201.10	147.237.76.34	United States	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
62.210.189.248	147.237.76.200	France	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

04-26-2016-00:04:03 to 04-26-2016-01:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
188.244.36.217	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
2.53.164.78	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
93.90.147.81	Sweden	147.237.72.156	aman.idf.il	drop	SAM rule	drop	12
155.254.215.27	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
155.254.239.21	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.254.65.211	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.150.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.33	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.160.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.35.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.11.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.151.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.50.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.186.214	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.150.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
188.244.36.217	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
2.55.13.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
213.57.210.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.20.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
68.81.223.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.84.219.66	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.136.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.77.33.197	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.11.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
36.99.31.82	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.98	United States	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
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
78.180.194.36	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 78.180.194.36	Block	6
78.180.194.36	Turkey	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	5
78.180.194.36	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	5
78.180.194.36	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.180.194.36	Block	5
78.180.194.36	Turkey	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	4
217.66.237.223	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
78.180.194.36	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.55.28.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.99.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.5.223.73	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
46.19.85.32	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
85.65.171.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/general/mobile	Block	1
199.30.24.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.248.174.4	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/xmlrpc.php	Block	1
67.19.79.218	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
87.70.84.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9704-he/refuah.aspx	Block	1
64.251.27.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.248.174.4	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/xmlrpc.php	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
109.160.160.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
84.94.35.70	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
77.126.27.218	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 77.126.27.218	Block	1
64.251.27.99	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on /robots.txt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/xmlrpc.php	Block	1
78.180.194.36	Turkey	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
213.57.210.204	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2617.jpg	Block	1
31.223.176.30	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.150.80	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.94.35.70	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.94.35.70	Block	1
77.126.27.218	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/	Block	1
89.248.174.4	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/xmlrpc.php	Block	1