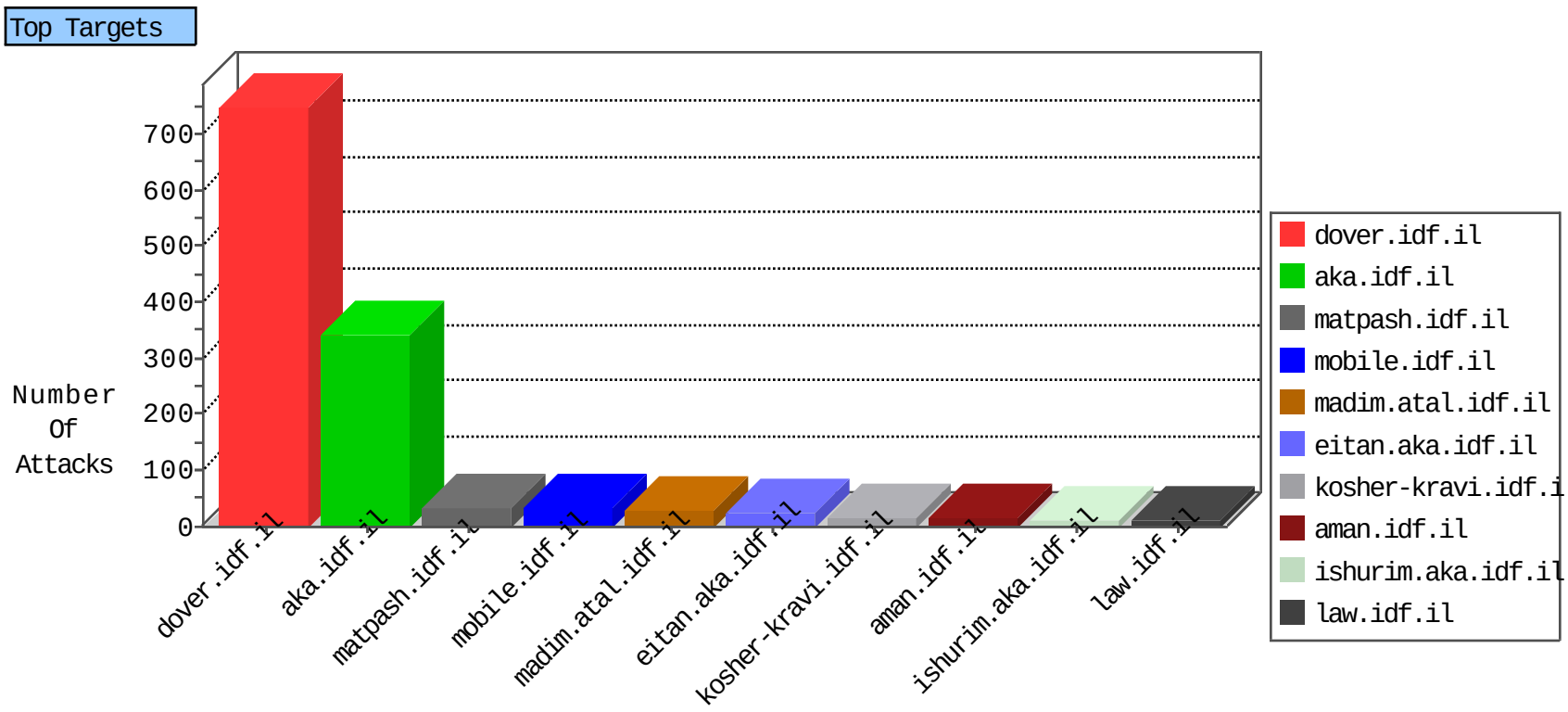
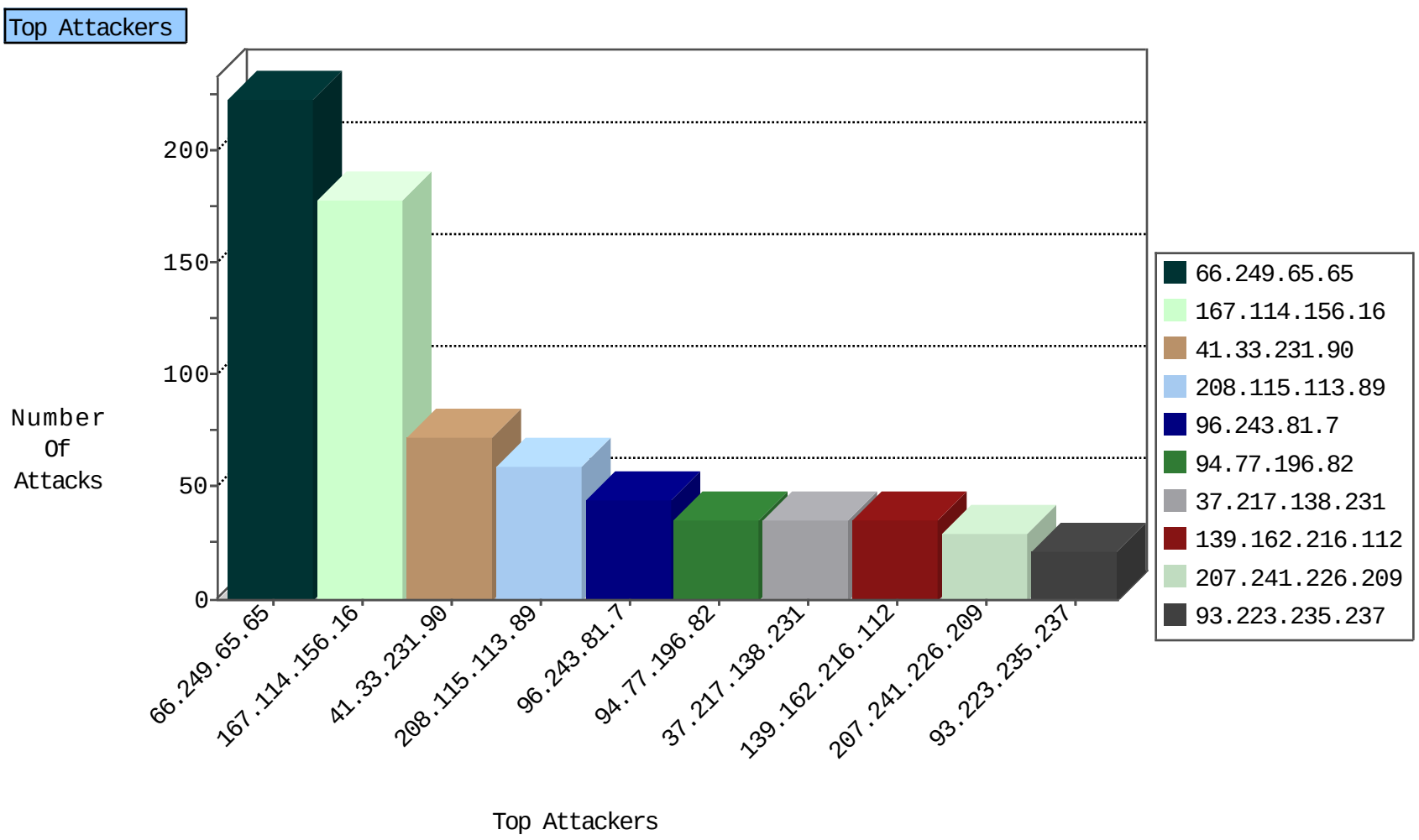
04-21-2016-23:04:08 to 04-22-2016-00:04:08

IDF Under Attack Daily Report





04-21-2016-23:04:08 to 04-22-2016-00:04:08

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	7892
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7561
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3167
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.29.223.39	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.217.138.231	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-21-2016-23:04:08 to 04-22-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-23:04:08 to 04-22-2016-00:04:08

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
188.120.148.132	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
124.105.9.3	147.237.76.148	Philippines	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 3072	1
66.102.6.191	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
23.96.109.87	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
201.173.131.218	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.124.35.115	147.237.76.201	Nicaragua	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.65.154.27	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
23.96.109.87	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
202.67.237.220	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN Potential SSH Scan	1
199.30.80.110	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
190.124.35.115	147.237.76.201	Nicaragua	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1

04-21-2016-23:04:08 to 04-22-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
96.243.81.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.217.138.231	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
207.241.226.209	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
93.223.235.237	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
176.228.53.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
207.46.13.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.14.176.28	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
5.22.135.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.182.26.77	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
192.115.83.5	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.120.24.234	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.115.83.5	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	7
37.26.148.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
206.74.212.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
173.168.204.88	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.146.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
104.131.147.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.9.246.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.137.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.145.219.91	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
41.242.136.4	Ghana	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.116.111.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.139	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
98.191.169.34	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.142.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.166.18	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
185.3.146.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
81.218.202.150	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.202.150	Block	5
5.29.53.108	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.53.108	Block	5
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	4
5.29.53.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
79.177.148.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.52.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.22.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.51.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.103.218	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12675-he/dover.aspx	Block	2
77.125.103.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.30.25.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
87.70.67.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8878-he/refuah.aspx	Block	1
46.222.165.152	Spain	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71929-he/	Block	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.175.165.144	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/â€Ž	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
203.133.168.224	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
109.64.9.27	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
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1926-he/cogat.aspx	Block	1
5.153.233.130	Sweden	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=571938da1ba492d3000; _pk_ref.20.8afc=%5B%22%22%2C%22%22%2C1461270748%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.20.8afc=10bbf50a40f85dd7.1460867723.2.1461270748.1461270748.; _pk_ses.20.8afc=*	Block	1
109.64.9.27	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.9.27	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
5.153.233.130	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=2	Block	1
5.29.6.182	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.228.19.67	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ar/â€Ž	Block	1
77.125.103.218	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
81.218.202.150	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/mobile	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method sionId=njzsdr55obpwfvf400foi53d; in URL __atuvc=2	Block	1
131.253.25.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-21-2016-23:04:08 to 04-22-2016-00:04:08