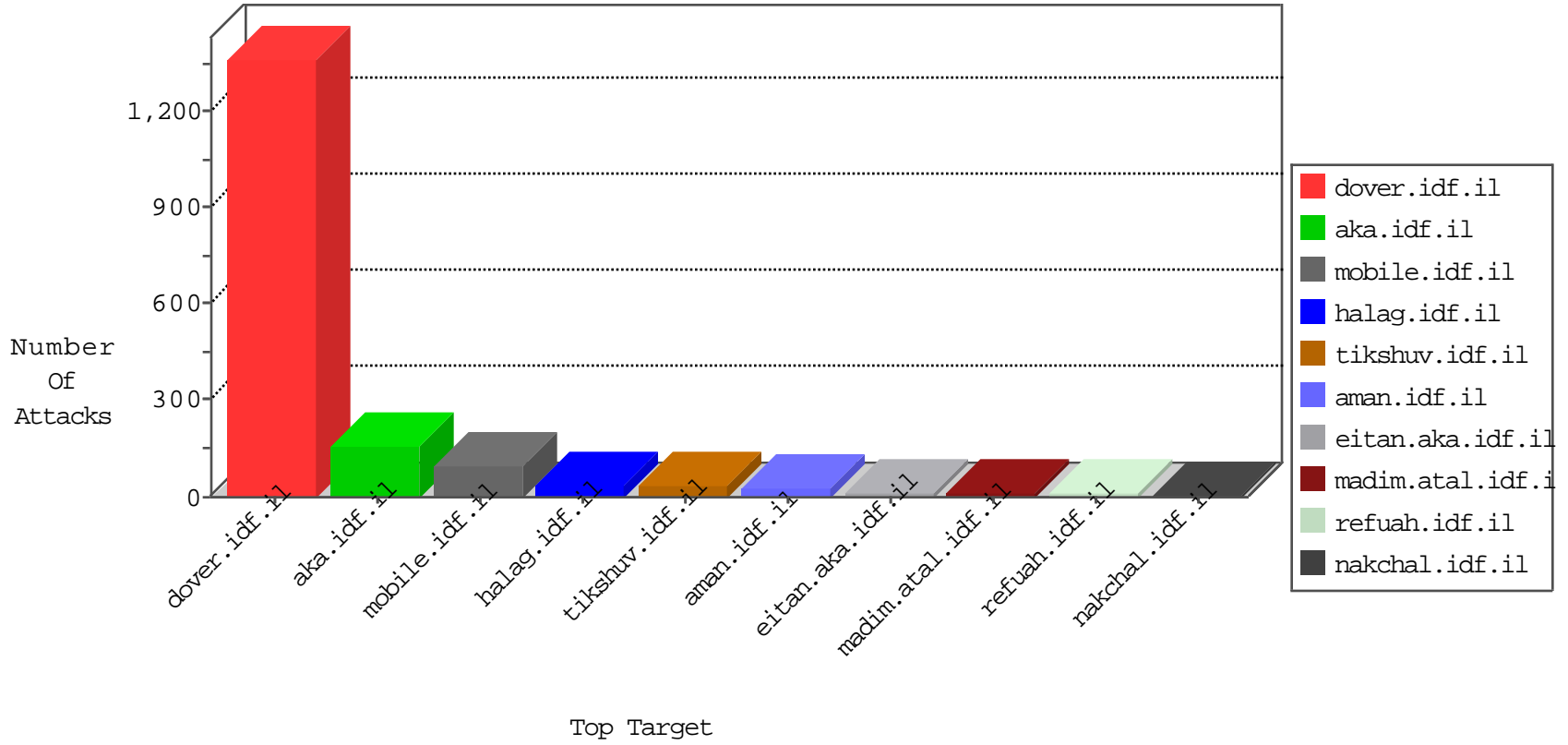


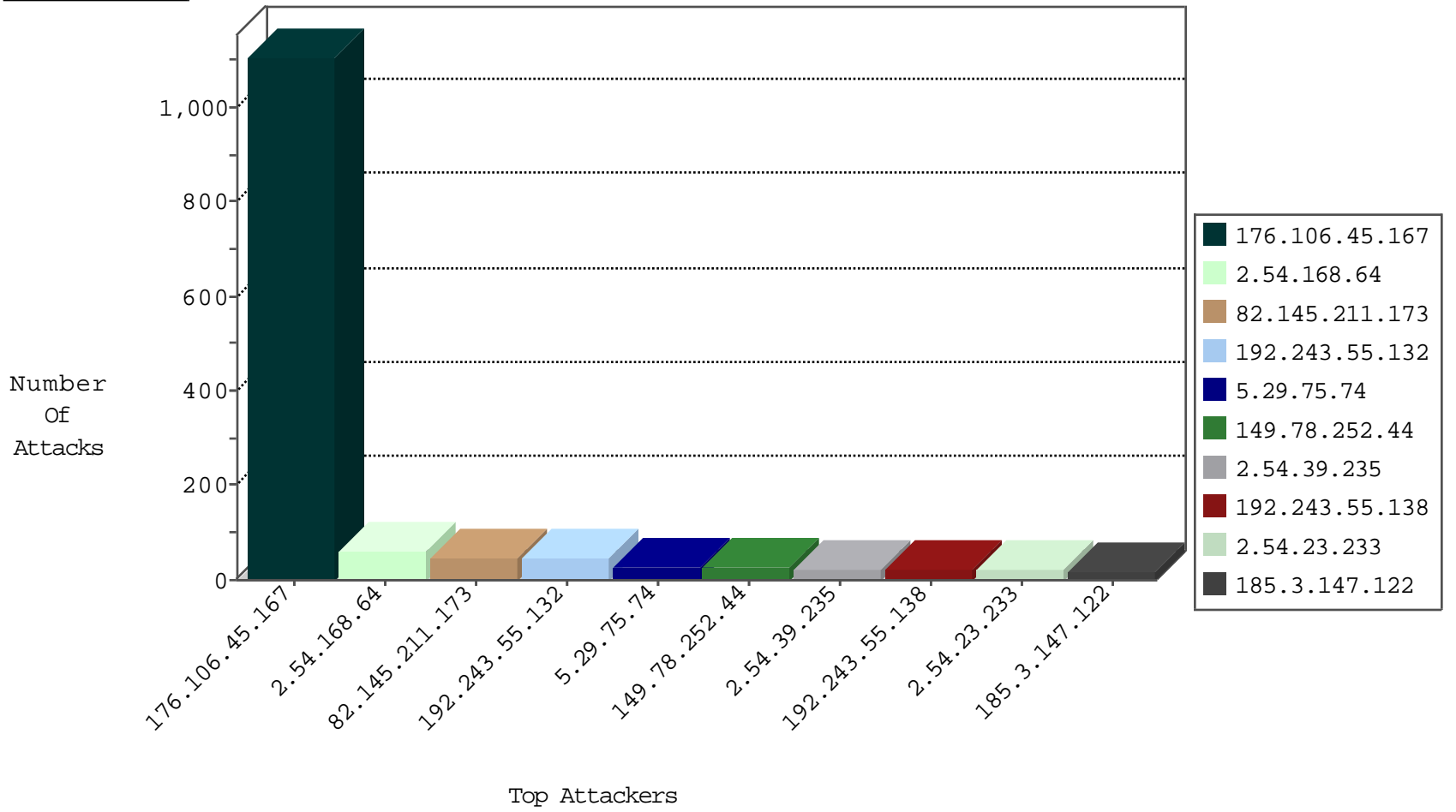
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1303
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	696
82.145.211.173	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	43
82.145.222.36	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
185.3.147.122	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
80.246.133.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.176	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
79.179.192.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.145.211.173	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
176.106.45.167	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
89.248.160.138	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
79.183.135.7	Israel	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
185.106.92.164		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Maieblackcat Security Scanner	Block	3
2.54.41.51	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
23.88.29.194	United States	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
173.247.228.10	United States	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Block	1
23.88.29.194	United States	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
185.106.92.164		147.237.76.39	mobile.meitav.idf.il	20085: HTTP: Maieblackcat Security Scanner Initial Request	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
31.162.86.86	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
185.106.92.164	147.237.76.39		mobile.meitav.idf.il	ET WEB_SERVER Muieblackcat scanner	1
115.29.197.215	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.162.86.86	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
31.162.86.86	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.162.86.86	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
186.208.65.232	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.199.51.251	147.237.76.197	Singapore	e.himush.idf.il	ET SCAN Potential SSH Scan	1
31.162.86.86	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
31.162.86.86	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
31.162.86.86	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.106.45.167	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	86
176.106.45.167	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.168.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.39.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.168.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.23.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
149.78.252.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
149.78.252.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.250.172.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.65.22	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.66	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.133.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
109.253.212.55	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.168.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.168.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.23.114	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.102.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.168.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.177.171	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.59.216	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.168.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
64.150.8.10	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.231.17	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.38.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.161	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.142.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
123.126.113.162	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.135.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.142.241.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.148.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.4.116	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
89.28.24.190	Moldova, Republic of	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.28.24.190	Block	5
89.28.24.190	Moldova, Republic of	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
2.54.39.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.23.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.23.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.168.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.202.112	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1
197.231.221.211	Liberia	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
37.205.24.154	Bosnia and Herzegovina	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.13.23.114	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
197.37.51.96	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.252.44	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.109.51.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.51.18	Block	1
207.46.13.182	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.205.24.154	Bosnia and Herzegovina	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
185.106.94.30		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8935-he/refuah.aspx	Block	1
197.37.73.69	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.241	Israel	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
149.255.208.117	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
84.109.51.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.64.124	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
207.241.229.151	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
40.77.167.14	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
103.41.177.26		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/) .html(	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.37.167.156	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.241	Israel	147.237.77.74	law.idf.il	Malformed URL __atuvs=56d9e9c1233c3832000	Block	1
156.205.98.131		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.39.201	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.39.201	Block	1
66.249.65.22	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
217.66.229.225	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.0.240.122	Tunisia	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
40.77.167.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
108.53.87.231	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.210.106	Block	1
197.41.193.193	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.241	Israel	147.237.77.74	law.idf.il	Unknown HTTP Request Method 7C9; in URL __atuvs=56d9e9c1233c3832000	Block	1
157.55.39.40	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.39.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyus/mazi.gov.il/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
197.0.240.122	Tunisia	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
41.34.210.192	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1