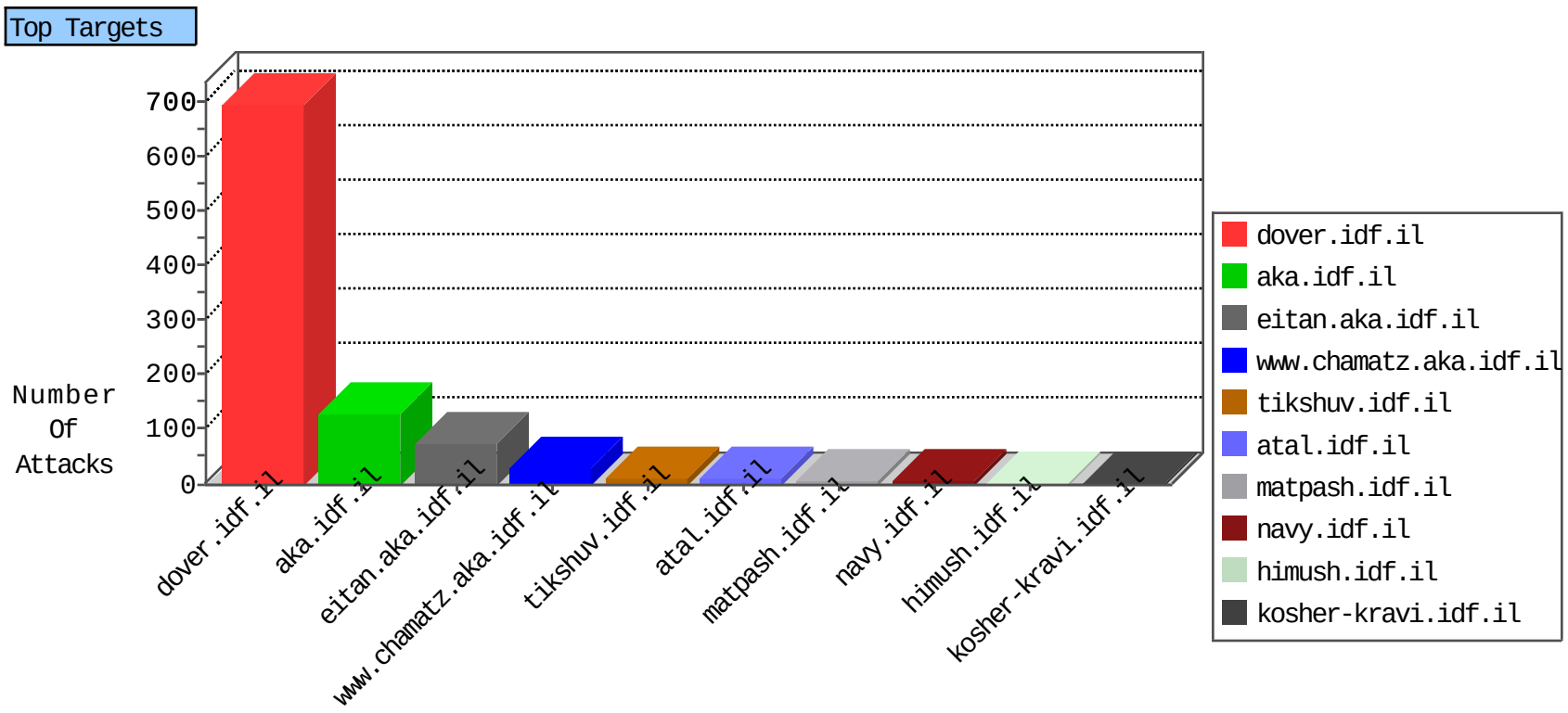
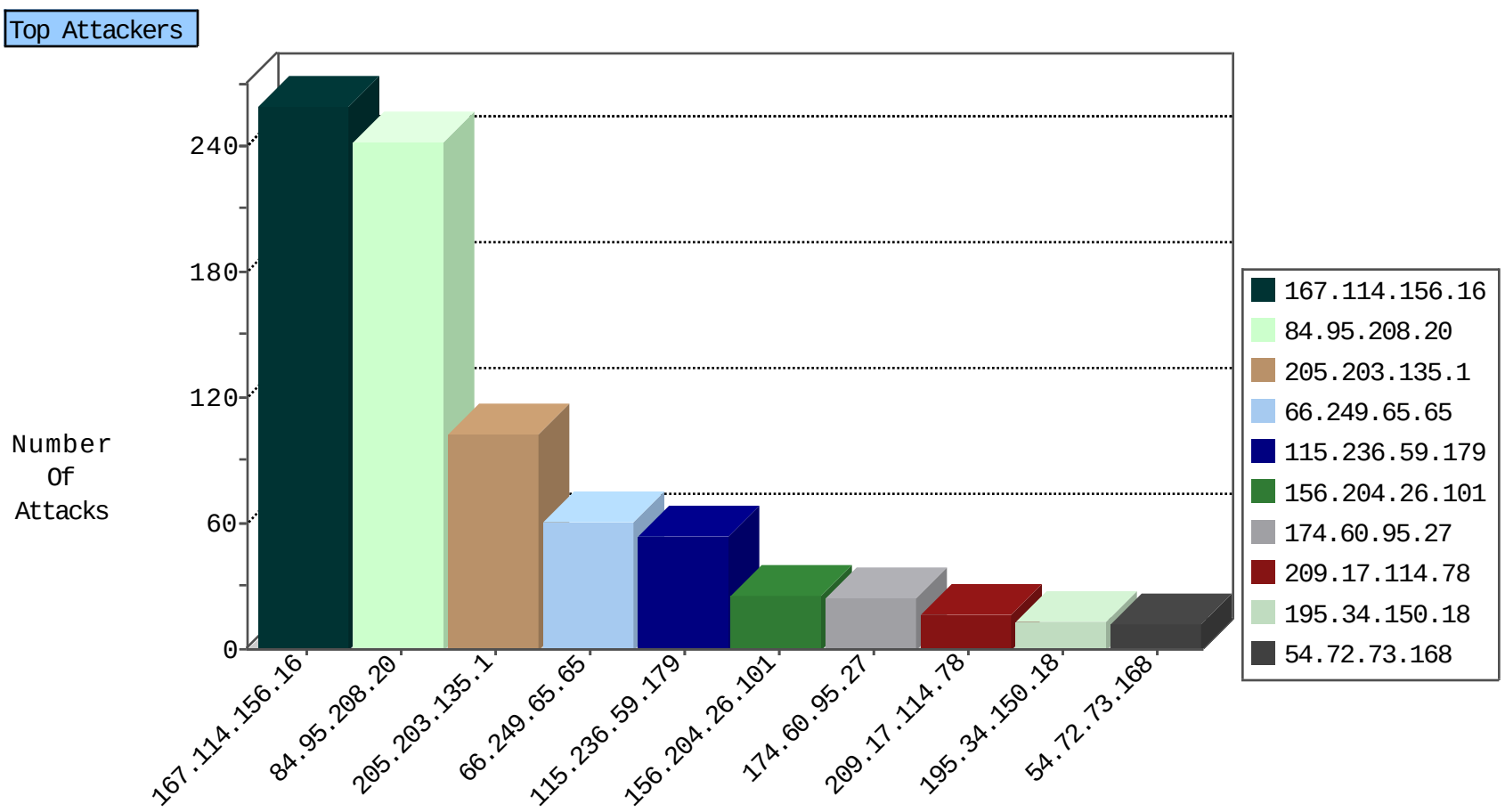
05-04-2016-03:04:00 to 05-04-2016-04:04:00

IDF Under Attack Daily Report



Top Target



Top Attackers

05-04-2016-03:04:00 to 05-04-2016-04:04:00

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	11677
115.236.59.179	China	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	997
156.204.26.101	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	924
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	532
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
107.150.46.36	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
123.59.59.52	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
94.102.49.116	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
107.150.46.35	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
94.102.49.116	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.102.52.10	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
107.150.32.60	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

05-04-2016-03:04:00 to 05-04-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-03:04:00 to 05-04-2016-04:04:00

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
115.236.59.179	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	3
189.70.136.195	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.24.43.14	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.197.232.40	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
120.24.43.14	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
115.236.59.179	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.214.25.64	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
41.185.26.175	147.237.77.176	South Africa	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
208.100.26.228	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

05-04-2016-03:04:00 to 05-04-2016-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
209.17.114.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
174.60.95.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.47.217.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
220.133.1.106	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
174.60.95.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
174.60.95.27	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
174.60.95.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.60.95.27	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
157.55.2.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
181.59.245.201	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.117.24.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.75.213.51	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.117.24.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.68.136.185	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.110	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
129.98.174.241	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.102.254.101	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.158	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.82	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.65.35.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.214.249.152	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
141.212.122.205	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.146	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Command Injection	command injection detected in URL: 'replace'	monitor	1
141.212.122.159	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.59.55.92	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
141.212.122.205	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	119
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	19
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
46.117.22.180	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 46.117.22.180	Block	7
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
129.98.174.241	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	3
66.249.84.172	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
54.148.35.147	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
46.117.22.180	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.117.22.180	Block	2
66.249.84.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.117.22.180	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/mobile	Block	2
66.249.84.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.31	Italy	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
37.187.56.47	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.187.56.47	Block	1
107.150.46.35	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.defences1.com/	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
220.255.146.54	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.89	Block	1
130.193.51.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
80.86.94.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	1
65.55.210.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.253.133.97	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.187.56.47	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
220.255.148.171	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
141.212.122.145	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
46.117.22.180	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/mobile	Block	1
80.86.94.7	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2662.jpg	Block	1
203.127.58.228	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.185.26.175	South Africa	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.122.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3350.jpg	Block	1
203.127.96.205	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.101.138.141	Germany	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
151.80.31.168	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.13.110.101	Ireland	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/1218-he/cogat.aspx-סיפור	Block	1
107.150.32.60	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.defences1.com/	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2799.jpg	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1