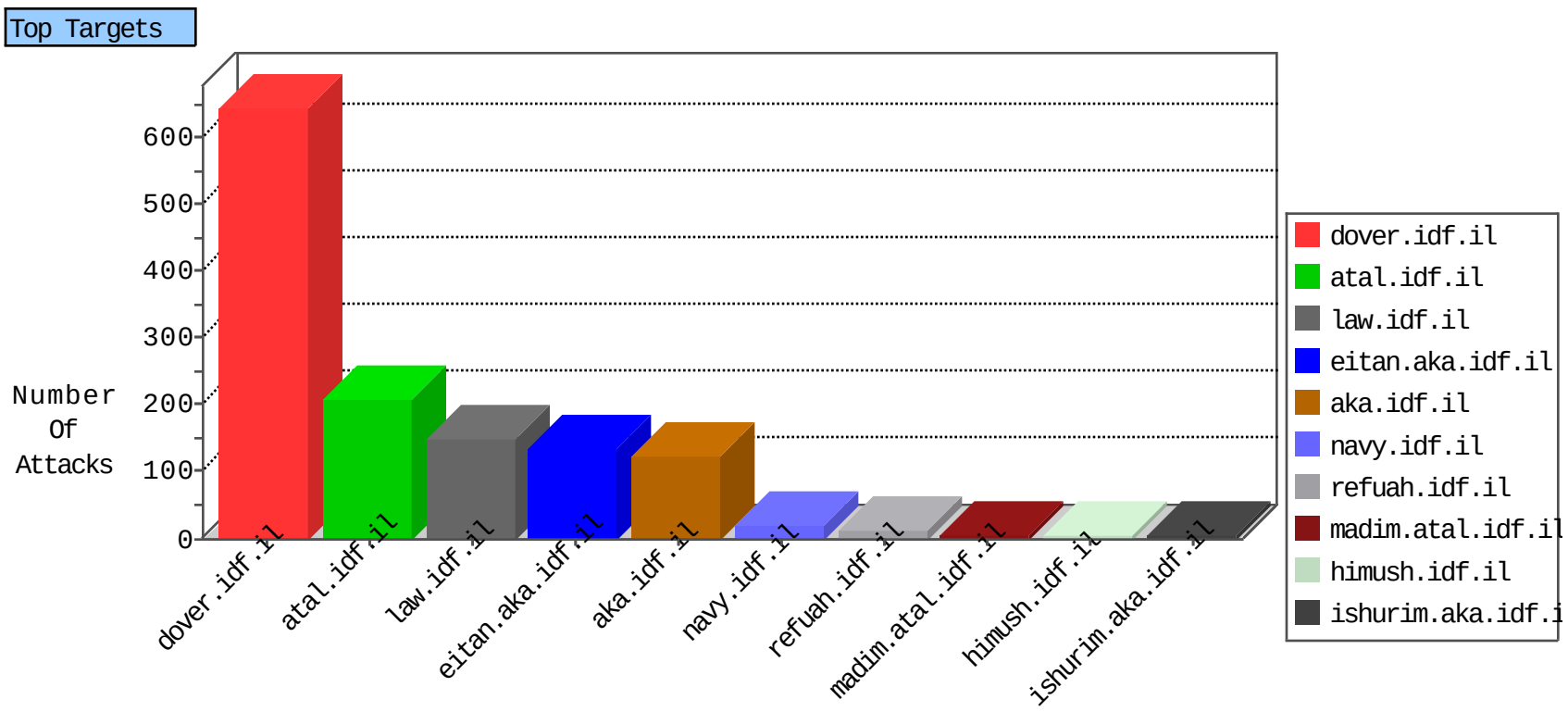
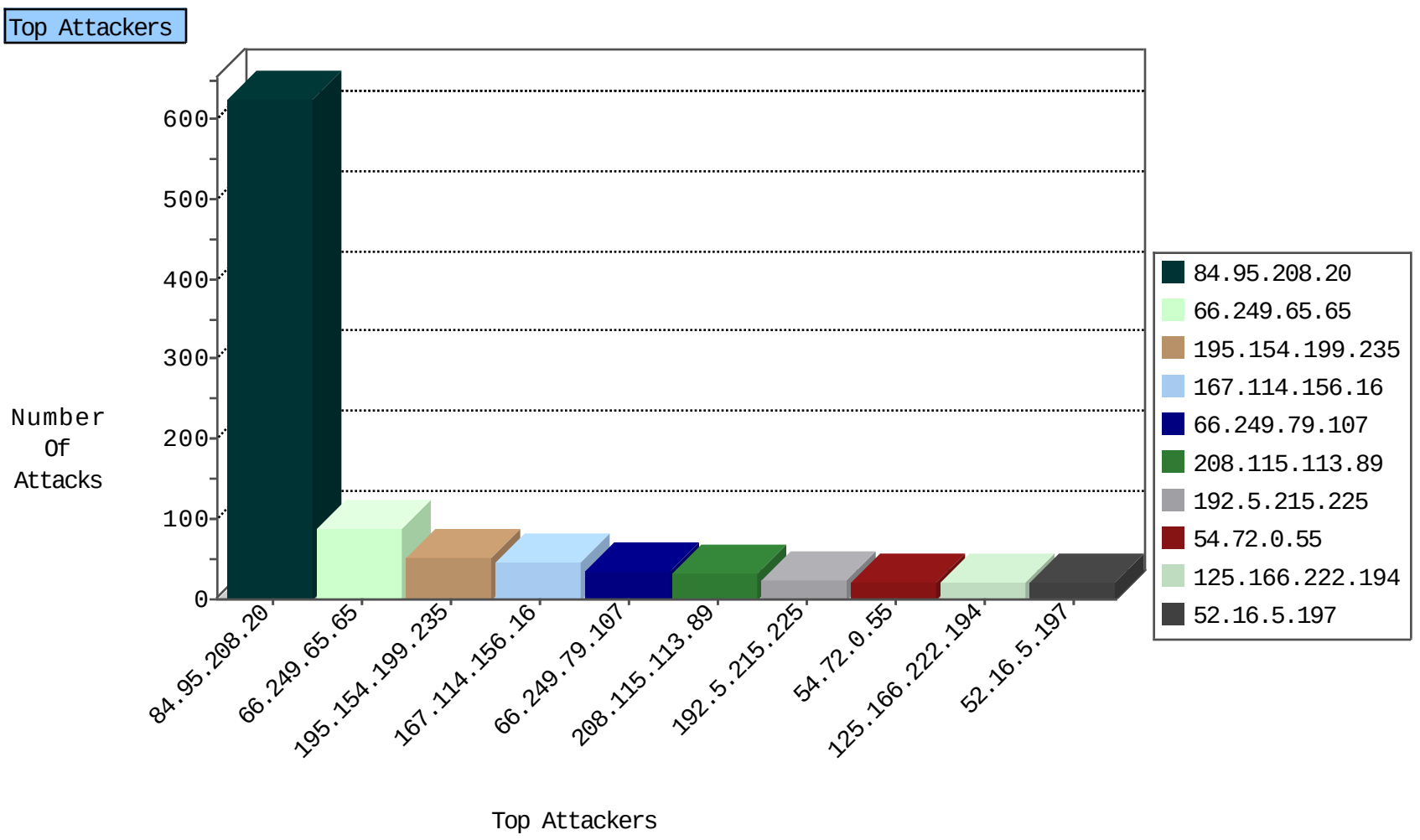
05-04-2016-05:04:06 to 05-04-2016-06:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2016-05:04:06 to 05-04-2016-06:04:06

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	2656
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	372
95.28.72.224	Russian Federation	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	130
89.178.65.165	Russian Federation	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	130
183.60.48.25	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
94.102.49.116	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.45	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.50	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

05-04-2016-05:04:06 to 05-04-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.143.180.166	United States	147.237.0.34	tikshuv.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

05-04-2016-05:04:06 to 05-04-2016-06:04:06

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
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.207.9.62	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.193.130.54	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
125.212.232.76	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.154	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
173.193.130.54	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
125.212.232.76	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
115.29.138.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
110.168.9.224	147.237.0.33	Thailand	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

05-04-2016-05:04:06 to 05-04-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	208
84.95.208.20	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	149
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	135
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	134
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
195.154.199.235	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
192.5.215.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
125.166.222.194	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
185.22.32.16	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.79.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
108.171.128.161	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.96.215	United States	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
213.57.248.132	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.248.132	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.79.107	United States	147.237.77.216	dover.idf.il	drop		drop	4
66.249.79.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
70.214.102.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.70.35	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
72.69.101.200	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
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
94.159.177.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
78.164.126.12	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.194.192.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.245.236.152	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.123.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
124.158.17.100	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.5	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.89	Block	2
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Malformed URL t…₪´¿„ˆnz3„g:ש6°,ÿסצ˛ ˛oף=]]62#[[€¡e¨™•f|טו<„[[61#]]מ¶[[#25]]lÊ[[#17]]¸€ü	Block	1
198.58.102.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.230.45	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀœ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ	Block	1
178.137.83.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀœ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ	Block	1
207.46.13.177	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/giyus/giyus/general.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	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/8/2278.jpg	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Parameter Name ₪[[†"#18[[]]#15….t ni]]₪´¿„ˆnz3„g:ש6°,ÿסצ˛ ˛oף=]]62#[[€¡e¨™•f|טו<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü	Block	1
184.155.13.172	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21149-he/dover.aspx	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]B¦#012•ÝÀbXdïMRìþn•Í¬£[[#27]]•{tÇ^Ý[[#5]]§*óõ¦p±\ïÀœ"ó[[#14]]¸¿–[[#22]]’ôI¹@RƒñÄbEÖ…¸Õ	Block	1
141.212.122.145	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	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/5/3295.jpg	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Query String ₪[[†"#18[[]]#15„¿´₪….t no]]ˆnz3„g:ש6°,ÿסצ˛ ˛oף=]]62#[[€¡e¨™•f|טו<„[[61#]]מ¶[[52#]]lÊ[[#17]]¸€ü	Block	1
195.154.199.235	France	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.83.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/doctor	Block	1
159.203.89.254	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
66.249.79.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1014-en/dover.aspx	Block	1
50.160.21.84	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL t…₪´¿„ˆnz3„g:ש6°,ÿסצ˛ ˛oף€¡e¨™•f lÊ[[#17]]¸€ü]]#25[[¶מ]]#16[[„<טו|=]]#26[[	Block	1
195.154.199.235	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/giyus/faq.aspx	None	1