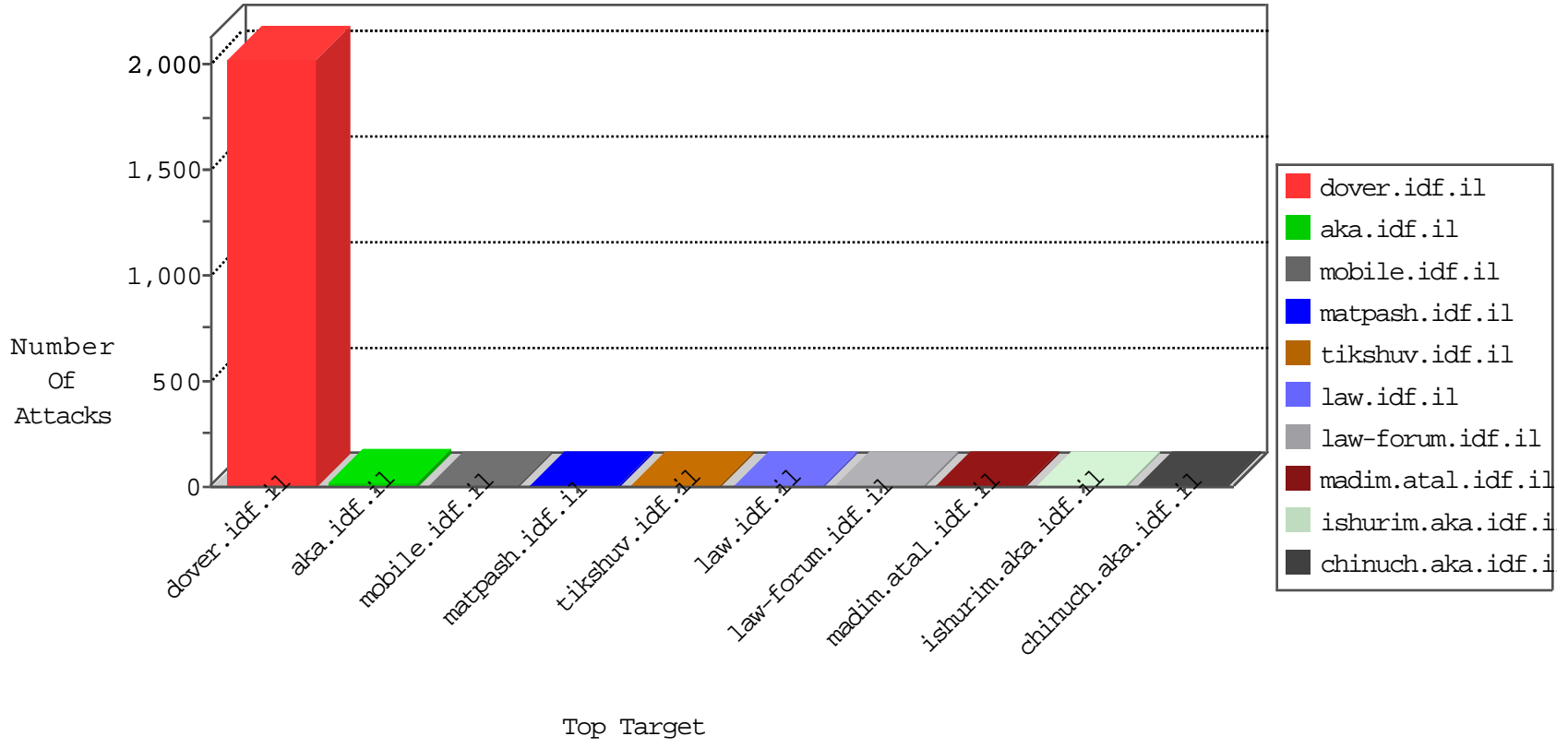


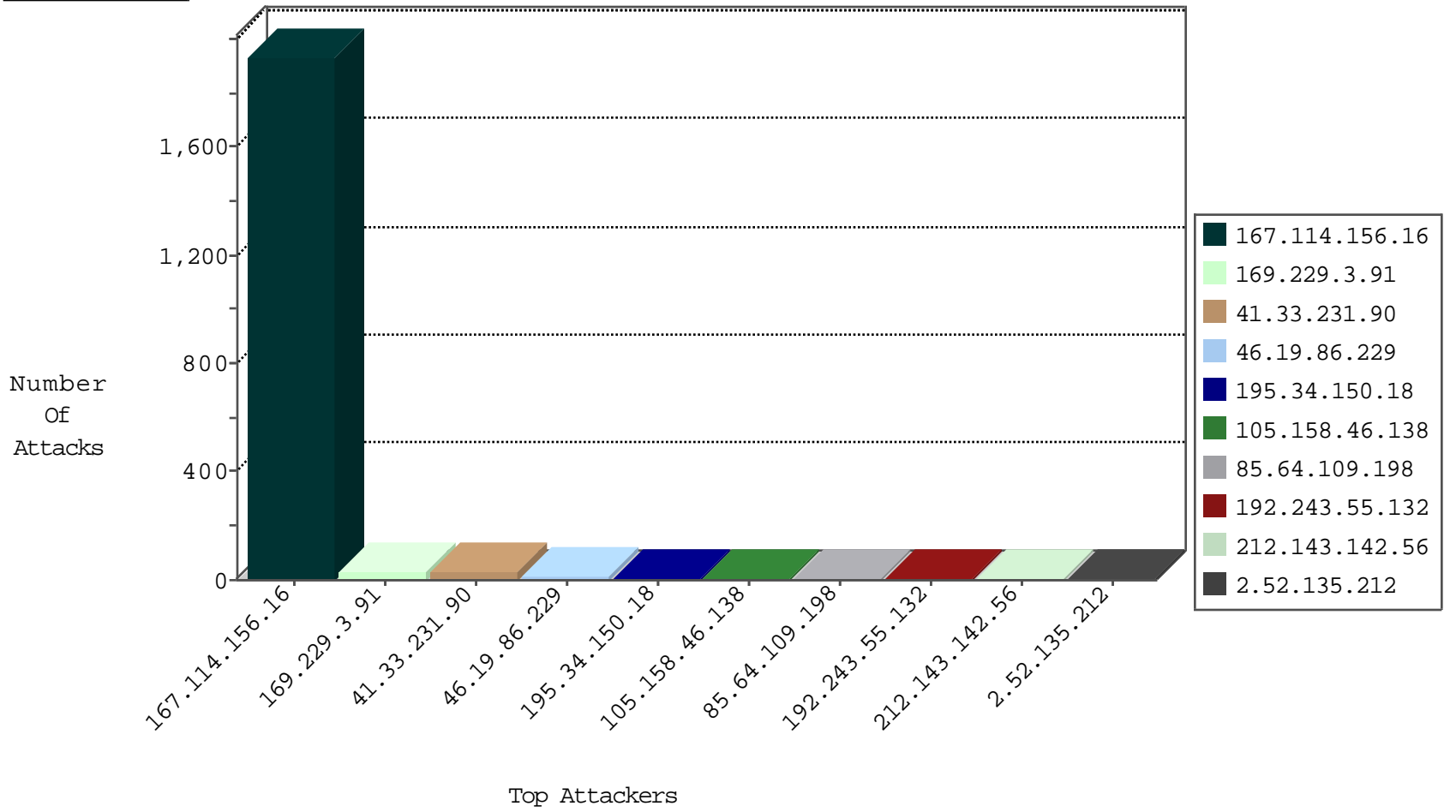
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3187
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2730
112.90.184.50	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
62.210.148.124	France	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
163.44.149.213	Japan	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
62.210.148.124	France	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## 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
93.174.93.10	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.216.3.174	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.193.2.8	147.237.77.212	France	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
73.17.14.46	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
201.69.168.112	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.101.60.86	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
105.158.46.138	147.237.77.176	Morocco	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
91.238.82.93	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.193.2.8	147.237.77.226	France	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.77.178	France	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
105.158.46.138	147.237.77.216	Morocco	dover.idf.il	Tehila - Perl LWP with fake user agent	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.86.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.108.29.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
85.65.116.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
66.249.64.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.90	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
83.45.118.82	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.135.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.85.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
69.140.155.89	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.203.218.135	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.91	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.100.86.100		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.135.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
158.255.6.220	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.81	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
73.17.14.46	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.135.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.93	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
85.65.116.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.120.125.4		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
159.203.218.135	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.88	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.23	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.52.135.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.94	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.109.198	Block	5
46.19.86.229	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
46.19.86.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
105.158.46.138	Morocco	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
81.218.201.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method bÃµÃ†[[#5]]Ã? in URL	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1737	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
146.0.32.85	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Unknown HTTP Request Method ÃŠÃ«Ã„Ã„5T{;W in URL æ°æ° çÖ»ÆfÖ·[[#11]]Ã-.[[#19]]	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Unknown HTTP Request Method #MÃ-Ã²ÃeÃ²[[#19]]MÃŠÃ~eG in URL	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/ikonim/pages/22122010tutim.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request request version	Block	1
207.46.13.10	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
105.158.46.138	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method ÃŠÃ«Ã„Ã„5T{;W	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-19706-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
5.79.68.161	Netherlands	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
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
105.158.46.138	Morocco	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3296.jpg	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name	Block	1
207.46.13.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
105.158.46.138	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Query String on æ°æ° çÖ»ÆfÖ·[[#11]]Ã-.[[#19]]	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method Af[[#5]]IÃ¾ÃªÃ°ÃªÃÆ	Block	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
105.158.46.138	Morocco	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL	Block	1
78.72.132.232	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version oYÃ«84Ã?[[#0]] \$Ã?Ã+W[[#14]]=Ãª<Ã;U[[#20]] [[#7]][[#8]]Ã¥ÃªÃª^8Ã„HÃŠ[[9Ã  Ã;Ã<	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.114	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
91.216.3.174	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in URL æ°æ°æçÖ»ÆfÖ·[[#11]]Ã-.[[#19]]	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method #MÃ-Ã²ÃeÃ²[[#19]]MÃŠÃ~eG	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1