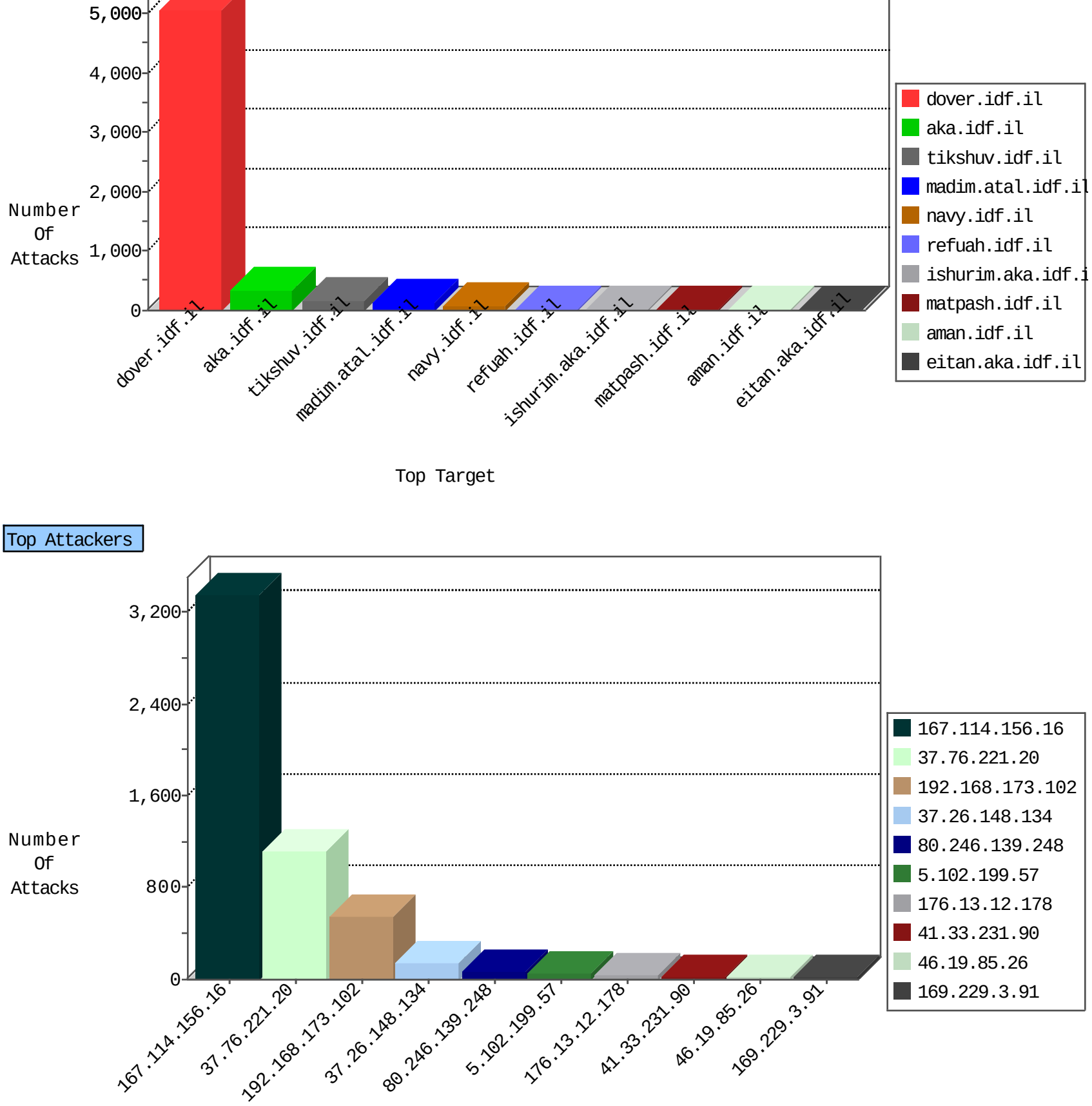
04-08-2016-13:04:05 to 04-08-2016-14:04:05

IDF Under Attack Daily Report



04-08-2016-13:04:05 to 04-08-2016-14:04:05

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	Block_Ip_Web_In	drop	3361
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	755
2.53.10.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	488
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	2
209.126.127.17	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.17	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
195.154.169.238	France	147.237.77.216	dover.idf.il	HTTP-MISC-drupal-SQLi-inc	dest-reset	1
204.42.253.2	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-13:04:05 to 04-08-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.42.56	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
176.228.201.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
217.55.71.27	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2
46.19.85.158	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

04-08-2016-13:04:05 to 04-08-2016-14:04:05

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	2
217.55.71.27	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
217.55.71.27	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	2
106.184.2.29	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
14.189.248.238	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
118.69.53.207	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
89.139.48.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-08-2016-13:04:05 to 04-08-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	361
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	194
37.26.148.134	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
39.9.156.7	Taiwan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
109.67.173.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
149.78.23.72	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.126.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.199.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.67.111.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.131.84.70	Greece	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.190	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.196.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.190	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.26	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.131.84.70	Greece	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.26	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.102.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.26	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
149.78.196.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
37.26.147.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.121.193.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.39.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.114.1.155	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.253.146.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.28.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.74.88.144	Belgium	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.25.53.71	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.22.134.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.23.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.2.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.129.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.135.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.68.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.14.160	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
80.246.139.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
5.102.199.57	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.102.199.57	Block	50
176.13.12.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
217.55.71.27	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.55.71.27	Block	9
14.154.19.240	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.154.19.240	Block	6
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.53.35.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
14.154.19.240	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
185.32.179.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.129.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
149.88.124.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.174	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
82.81.95.154	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
54.153.33.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
93.172.169.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method YÃÄ in URL ¦<;ß†‰a²x[[#19]]ע #[[#24]][[#15]]lž»»¯®ßÝ;¢¯•dÐßɔ.„	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Query String on 9mƥfƥ„”ž	Block	1
41.109.143.210	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.122	Block	1
208.115.125.36	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
84.109.224.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
62.219.192.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method YÃÄ	Block	1
5.102.199.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.not	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in URL	Block	1
95.86.118.25	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
217.55.71.27	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Malformed URL 9mƥfƥ„”ž	Block	1
41.140.204.77	Morocco	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1038-en/dover.aspx parameter ctl00$ContentPlaceHolder1$txtEmail	Block	1
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
213.57.178.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.13.253	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Query String on ¦<;ß†‰a²x[[#19]]ע #[[#24]][[#15]]lž»»¯®ßÝ;¢¯•dÐßɔ.„	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
5.157.57.61	Sweden	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
109.64.133.193	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	1
217.132.106.9	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8992-he/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19689-he/kkkkkkk=17a07365kkkkkkk_17a07365	Block	1
79.183.110.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
5.22.131.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sahar	Block	1
157.55.39.122	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.122	Block	1
213.233.64.162	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1