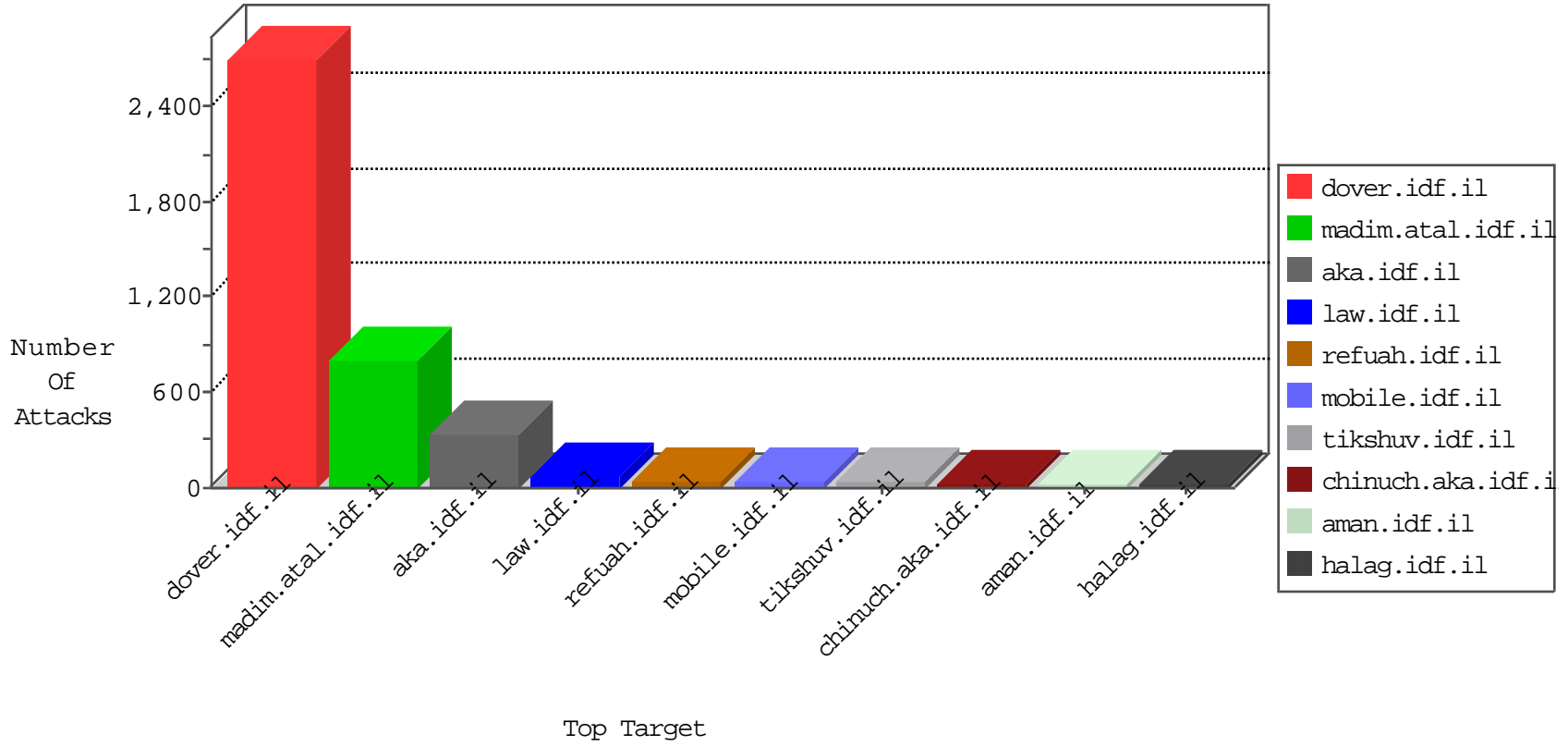


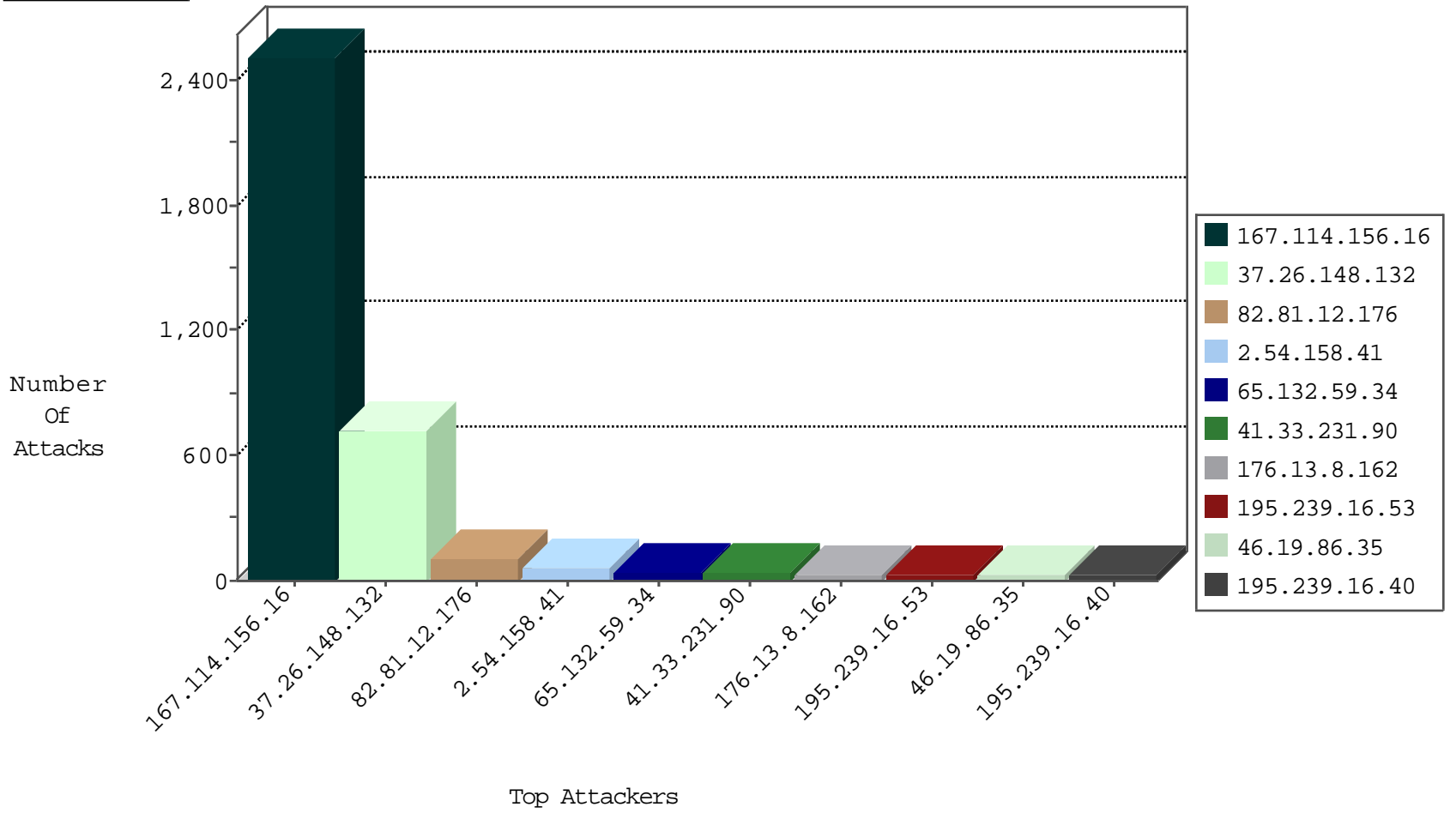
# IDF Under Attack Daily Report



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	3068
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
208.73.206.244		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
66.102.9.21	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
194.58.185.52	Russian Federation	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.34	yochalan.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.246.230.40	China	147.237.77.233	atal.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
204.12.168.26	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
185.130.5.247		147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.247		147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
88.150.221.26	United Kingdom	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.195	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
172.245.218.130	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
185.130.5.247		147.237.0.19	madim.atal.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	1
208.98.56.66	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.148.132	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
204.12.168.26	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	4
85.233.76.49	147.237.0.34	Russian Federation	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	2
197.157.244.243	147.237.76.86	Somalia	navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.247	147.237.77.216		dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
112.168.26.199	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
197.157.244.243	147.237.76.177	Somalia	ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
112.168.26.199	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
219.128.162.66	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	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	36
176.13.8.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.157.236	Israel	147.237.76.147	chimuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.177.0.54	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.147.168	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.66.113.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
92.8.60.233	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.121.158	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.192	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
31.210.186.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.236.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.129.21.51	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.8.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.167.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
89.138.13.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.159.167.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
94.159.167.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
149.78.233.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.107.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	5
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
92.229.162.244	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.165	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.129.21.51	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.38.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.26.149.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
104.131.147.112	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
212.199.121.158	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.65.157.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.193.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.100.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.220.34	Israel	147.237.76.147	chimuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.254.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.220.34	Israel	147.237.76.147	chimuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.198.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.70.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.105.99	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
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	449
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.148.132	Block	237
2.54.158.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.201.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	6
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	6
213.8.204.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	6
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	6
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	5
79.180.176.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
87.68.164.90	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.164.90	Block	4
149.50.122.75	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.68.58.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.173.183.102	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 93.173.183.102 (Unknown SSL Session)	None	2
84.108.86.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.233.76.49	Russian Federation	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	2
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.35	Block	2
109.66.188.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.233.76.49	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-admin/admin-ajax.php	Block	2
46.19.86.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	2
213.57.137.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	2
172.245.218.130	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 172.245.218.130	Block	2
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
65.132.59.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
2.54.30.229	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
89.38.150.47	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
85.233.76.49	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 85.233.76.49	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.9.46	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.123.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1
87.68.164.90	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
46.120.156.193	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
172.245.218.130	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/cgi-bin/php5	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
109.66.113.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.38.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.13.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.65.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7661-he/nakchal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.180.97.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.205.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.183.102	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1