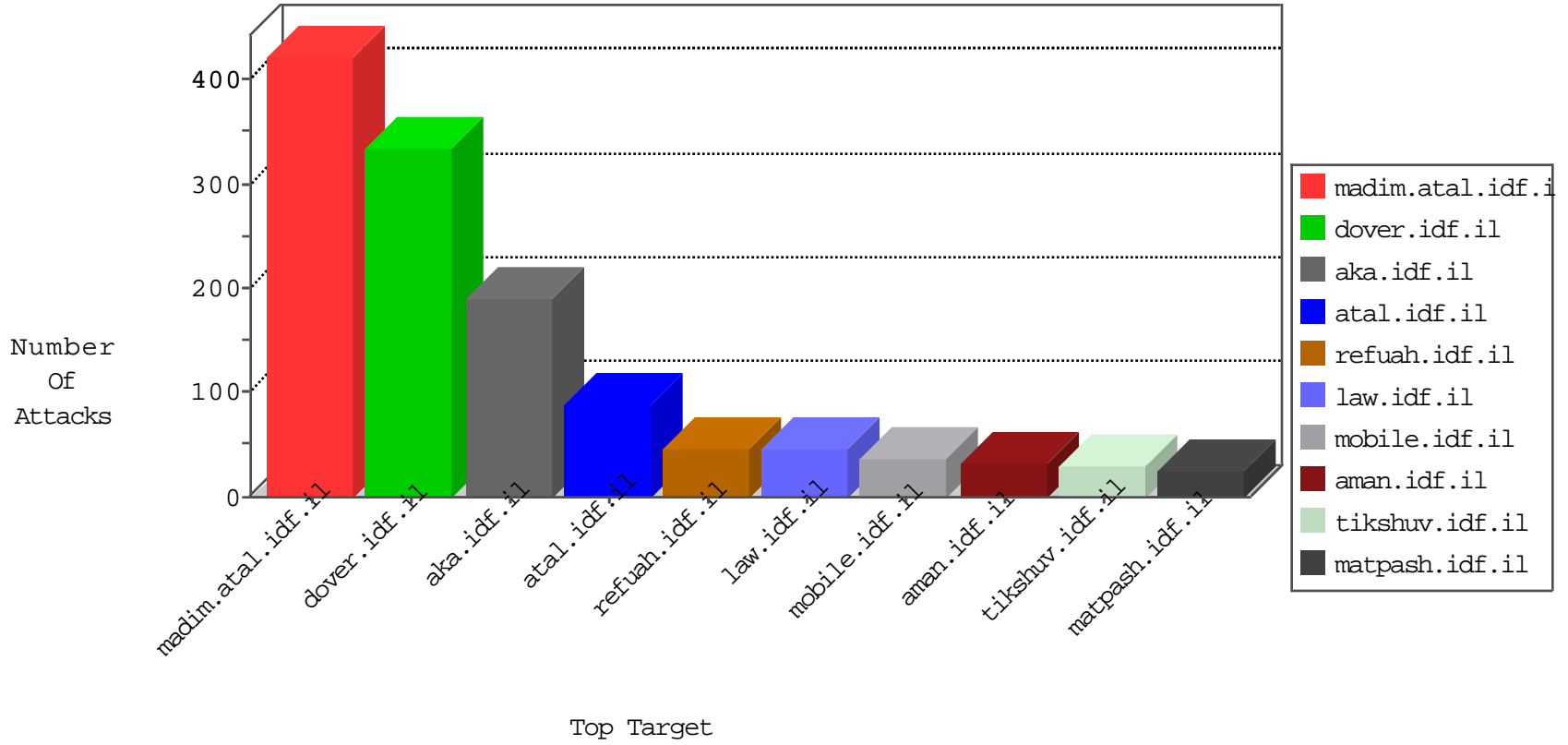


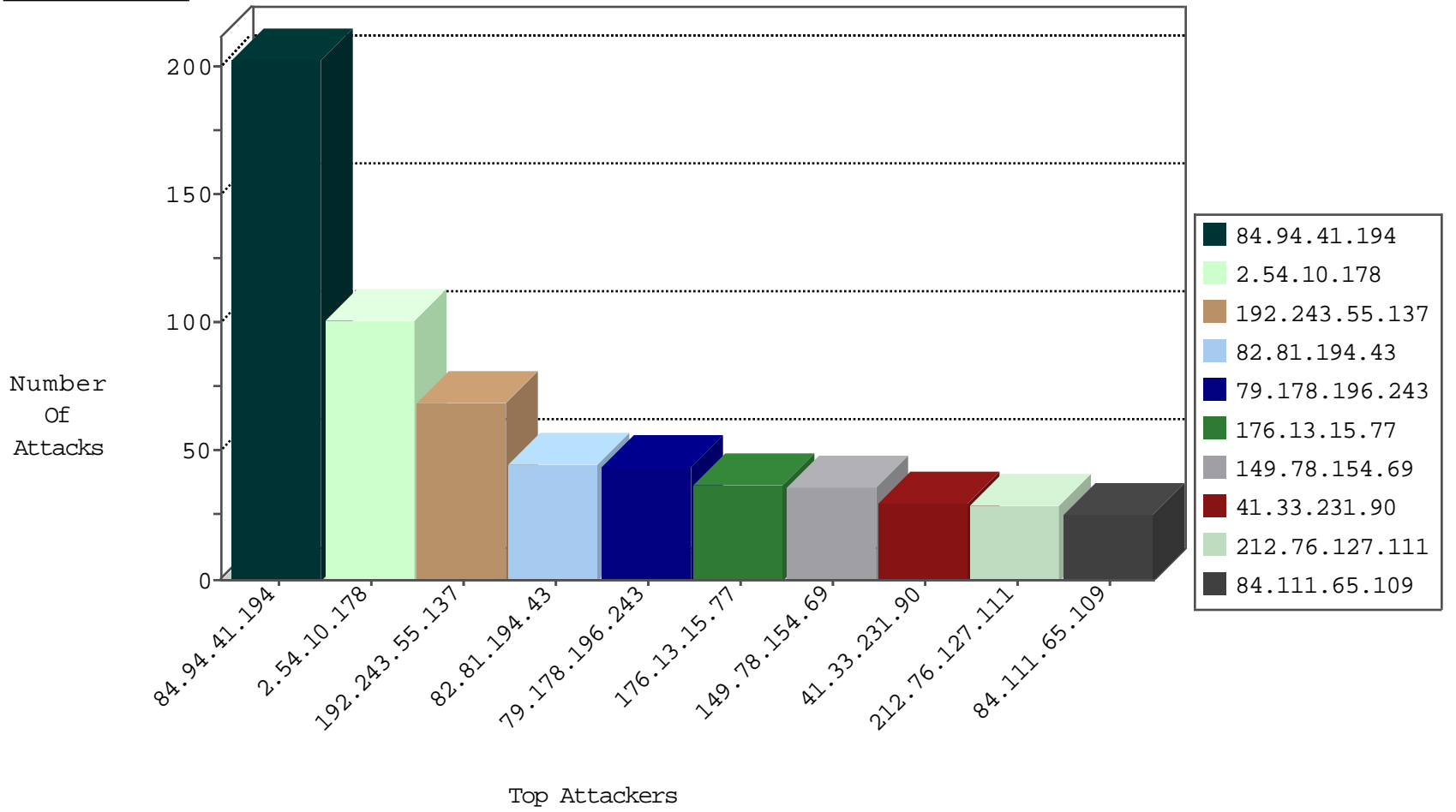
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
40.77.167.38	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
69.171.230.106	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.200.159	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
84.109.39.112	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
84.108.245.177	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
79.183.33.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
80.178.195.79	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.206	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

## 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	3
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
182.254.149.138	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.223.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.125.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
213.8.44.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
2.52.4.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.253.141.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.35.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.252.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
2.54.134.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	29
107.167.103.61	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
93.172.239.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
2.54.40.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
77.246.55.136	Zimbabwe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
79.178.196.243	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.178.196.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.178.196.243	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
176.13.10.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.164.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.181.13.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.191.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.148.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.9.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.180.125.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.196.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.195.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.196.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.178.196.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
77.246.55.136	Zimbabwe	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
212.199.57.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.57.222.64	France	147.237.72.166	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
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.195.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.22.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.7.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
80.178.169.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.191.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.13.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.52.7.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
207.46.13.2	United States	147.237.77.243	mobile.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
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.54.10.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
82.81.194.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
84.111.65.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.54.10.178	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.10.178	Block	20
185.13.194.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	18
185.27.106.70	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	17
79.182.100.186	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 79.182.100.186	Block	14
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
109.253.146.85	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.146.85	Block	5
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
64.233.173.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
64.233.173.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.119.117.85	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
64.233.173.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.146.85	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
79.181.15.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.211.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.226.55.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$35 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.16.86	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.132.65.140	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
199.30.24.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.172	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.13.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$117 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
79.178.108.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
93.172.239.216	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
82.80.160.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$1 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
213.151.47.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/71180.pdf&sa=u&ved=0ahukewi46d3y5ihlahxivrqkhr-_cvqqfggyamac&usq=afqjcnfpq4zu0hidypmzngz4wcvri0y8ha	Block	1
79.182.174.30	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
184.168.192.163	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/xmlrpc.php	Block	1
109.226.55.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$45 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
220.181.108.78	China	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.111.22.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×ç×ÿ×~×*×"	Block	1
199.30.24.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.164.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.13.77	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$71 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.220.155.215	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/45741.pdf&h=8aqhgugjc	Block	1
103.16.228.98	Hong Kong	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
46.120.126.198	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$117 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
216.144.237.118	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
79.182.174.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.83.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.62.131.192	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1