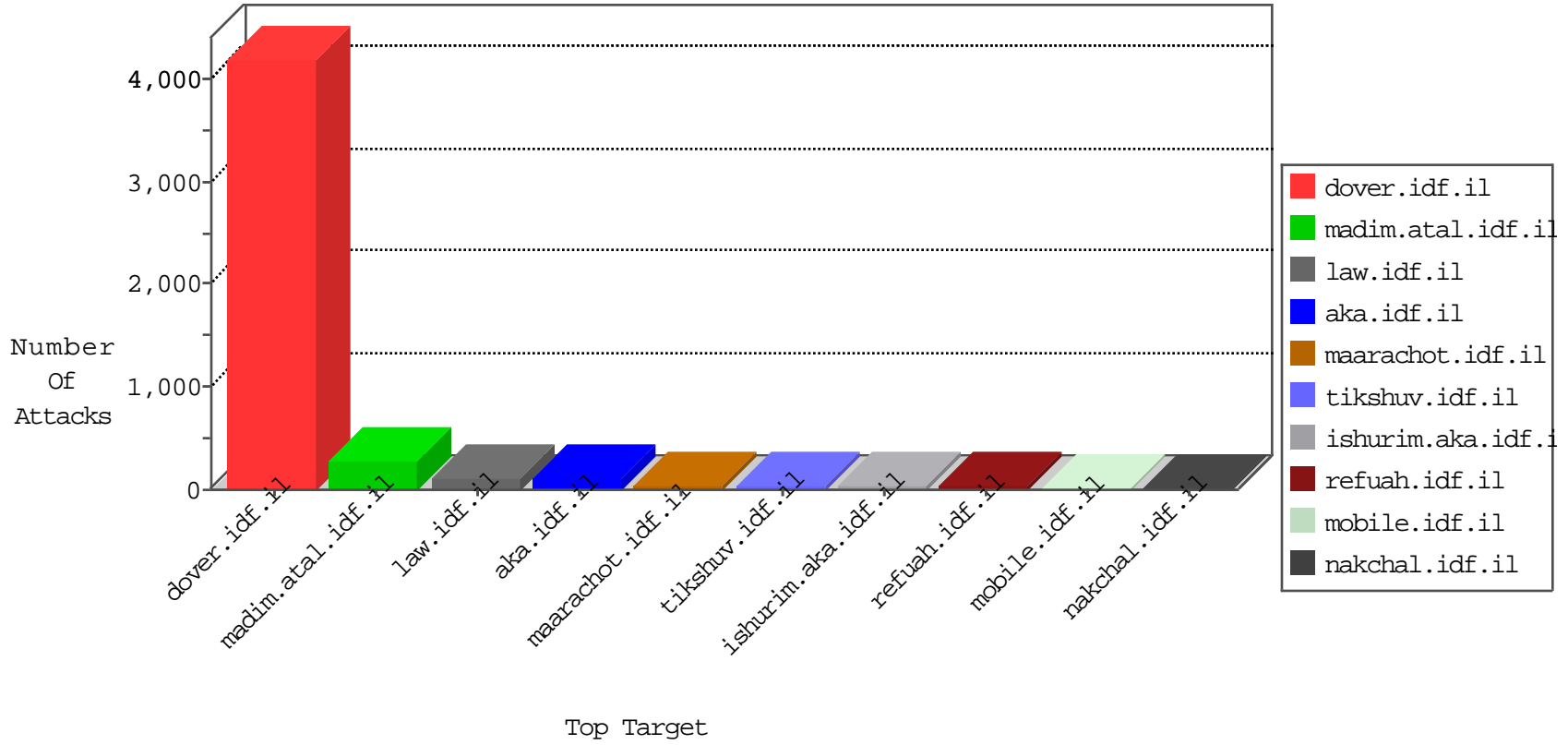


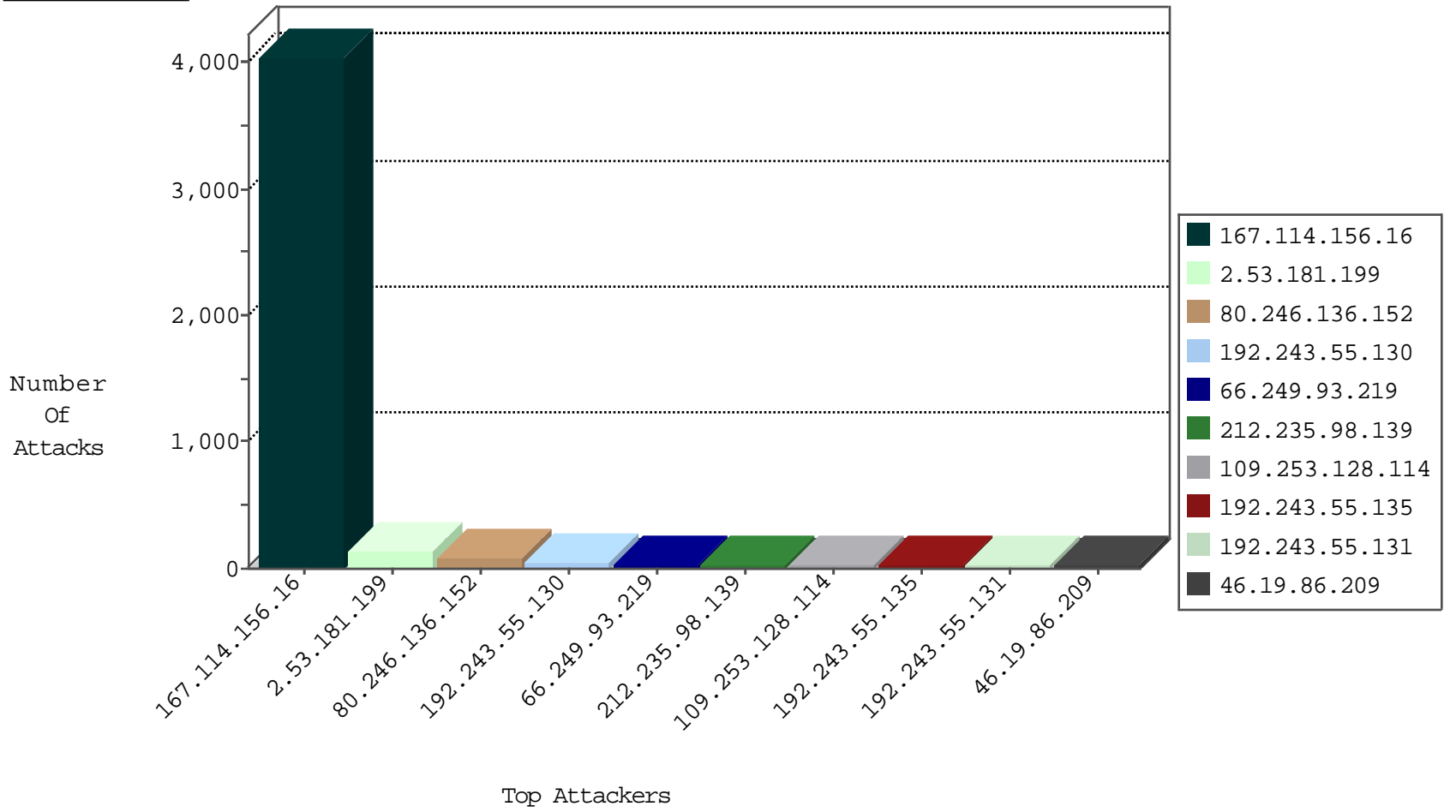
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4045
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
2.53.61.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
213.57.108.74	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.67	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
216.218.206.91	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.67	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.194.189	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
81.218.135.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.172	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.219	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	36
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.151.52.139	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.9.213	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
118.163.79.156	147.237.77.121	Taiwan	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.172.173	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.163.212.37	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.226.105.211	147.237.0.34	France	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	1
1.53.67.22	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.8.204.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.173	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.163.212.37	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
79.178.18.99	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
87.70.33.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.67.176.111	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
85.130.131.116	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.22.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
80.246.139.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.252	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
46.19.85.252	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.131.116	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
188.161.20.83	Palestinian Territory Occupied	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
95.35.10.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.130.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.131.116	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
176.13.6.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.28.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.96.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.22.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.116.177.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.120	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
2.53.181.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
80.246.136.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
109.253.128.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.197.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.147.195	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakchal.idf.il/1119-he/nakhal.aspx	Block	2
131.253.25.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.133.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.200	Block	2
85.64.104.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.104.160	Block	2
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.200	Block	2
87.70.33.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	2
46.226.105.211	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/wp-login.php	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 5qufj in URL	Block	1
157.55.39.199	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
91.108.88.189	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
39.36.31.248	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
2.55.53.131	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.200	Block	1
128.232.110.28	United Kingdom	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.176.111	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.129	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.55.130.138	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.130.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.9.53	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.200	Block	1
85.64.104.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
176.13.22.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.55	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.186.191.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
5.29.162.249	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.65.241	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/webservices/wscity.aspx	Block	1
157.55.39.120	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9641-he/refuah.aspx	Block	1
2.53.156.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.227.66.92	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/487-he/patzar.aspx	Block	1
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=570de12018d3a5a7000	Block	1
37.26.146.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captchaText in www.aka.idf.il/main/gyus/default.aspx	None	1