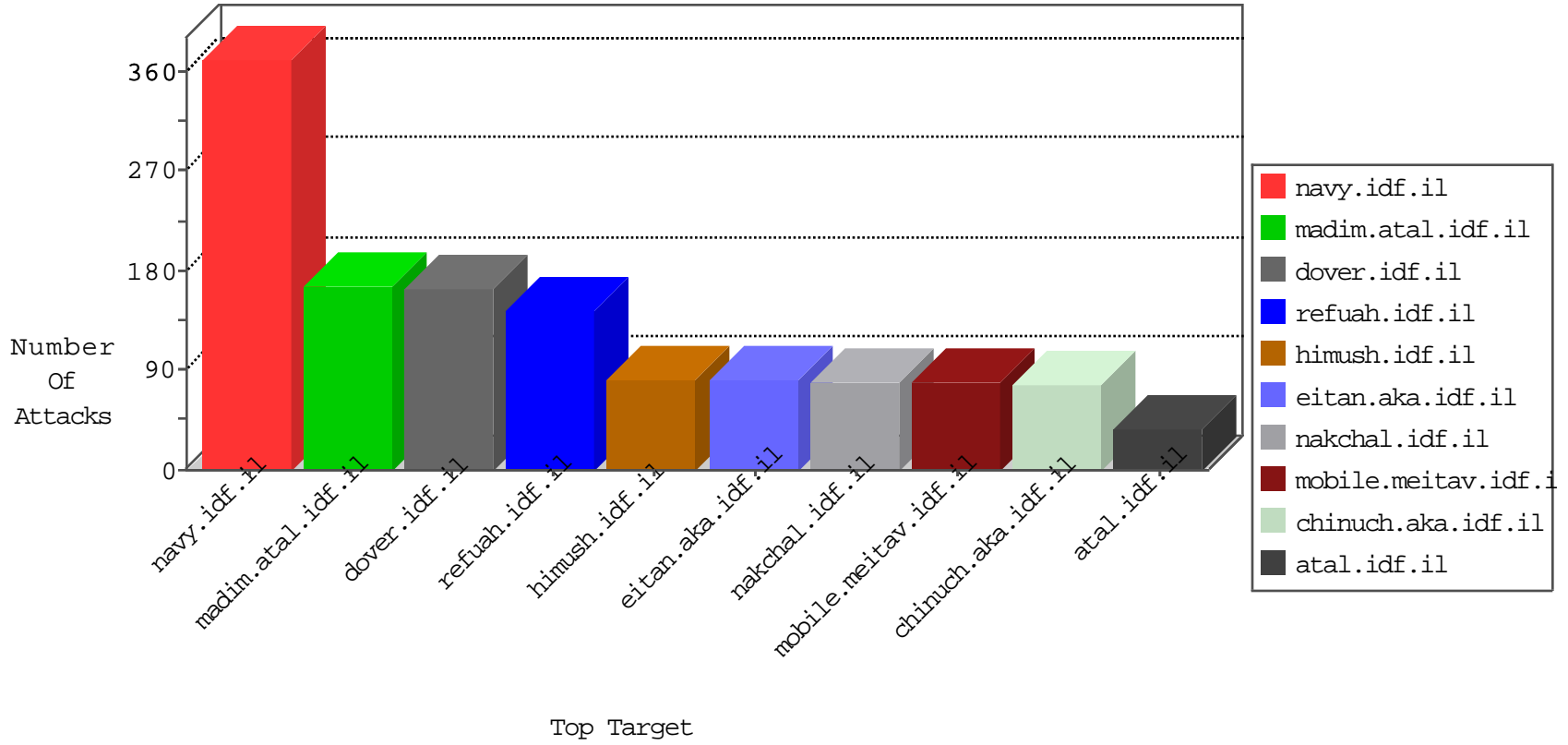


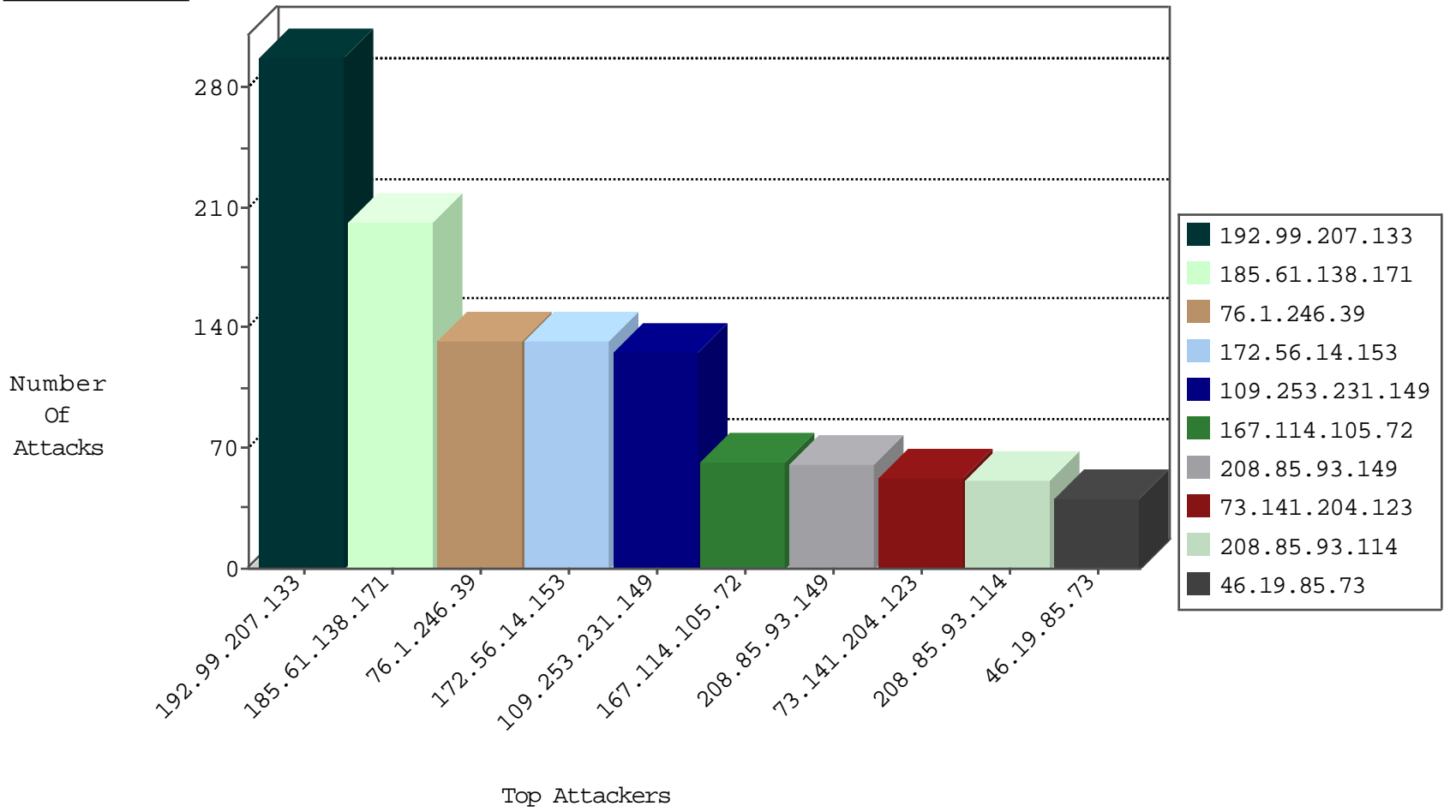
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
60.246.170.29	Macau	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
117.21.248.87	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Top	drop	1
209.126.136.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.186	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
45.79.111.169	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
117.21.248.87	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.10	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.67.13	147.237.76.148	United Kingdom	ggqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
163.172.67.13	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
117.21.248.87	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.47.12.162	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.52.97.91	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
94.102.48.195	147.237.76.148	Netherlands	ggqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.67.13	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
150.242.238.99	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.56.14.153	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	133
167.114.105.72	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	61
73.141.204.123	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	53
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	31
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	31
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
185.61.138.171	Ukraine	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
185.61.138.171	Ukraine	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
185.61.138.171	Ukraine	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
185.61.138.171	Ukraine	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
185.61.138.171	Ukraine	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
185.61.138.171	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
185.61.138.171	Ukraine	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
62.0.76.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
185.61.138.171	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
76.1.246.39	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
76.1.246.39	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
76.1.246.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
76.1.246.39	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
76.1.246.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
76.1.246.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
76.1.246.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
76.1.246.39	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
172.56.26.217	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.3	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
208.85.93.114	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.85.93.114	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.85.93.114	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.85.93.114	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.0.76.227	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
208.85.93.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.99.207.133	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.231.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
109.253.206.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.19.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.15.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 45.79.111.169	Block	2
80.178.98.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 45.79.111.169	Block	2
157.55.39.226	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.aspx/getjs	Block	2
70.209.128.183	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 45.79.111.169	Block	2
176.13.249.136	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
66.249.64.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9269-he/dover.aspx	Block	1
66.249.79.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.86.240	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
2.53.6.4	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.169.7.223	United States	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for 147.237.77.235/	Block	1
66.249.64.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1
46.19.86.240	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method qqxv2qx55 in URL	Block	1
2.55.170.16	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	1
212.199.49.169	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
70.214.64.141	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
62.0.76.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.26.147.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
109.95.19.184	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3470.jpg	Block	1
75.63.29.234	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
62.0.101.97	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.0.101.97	Block	1
66.249.79.143	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2341.jpg	Block	1
46.19.86.132	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
180.76.15.158	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1