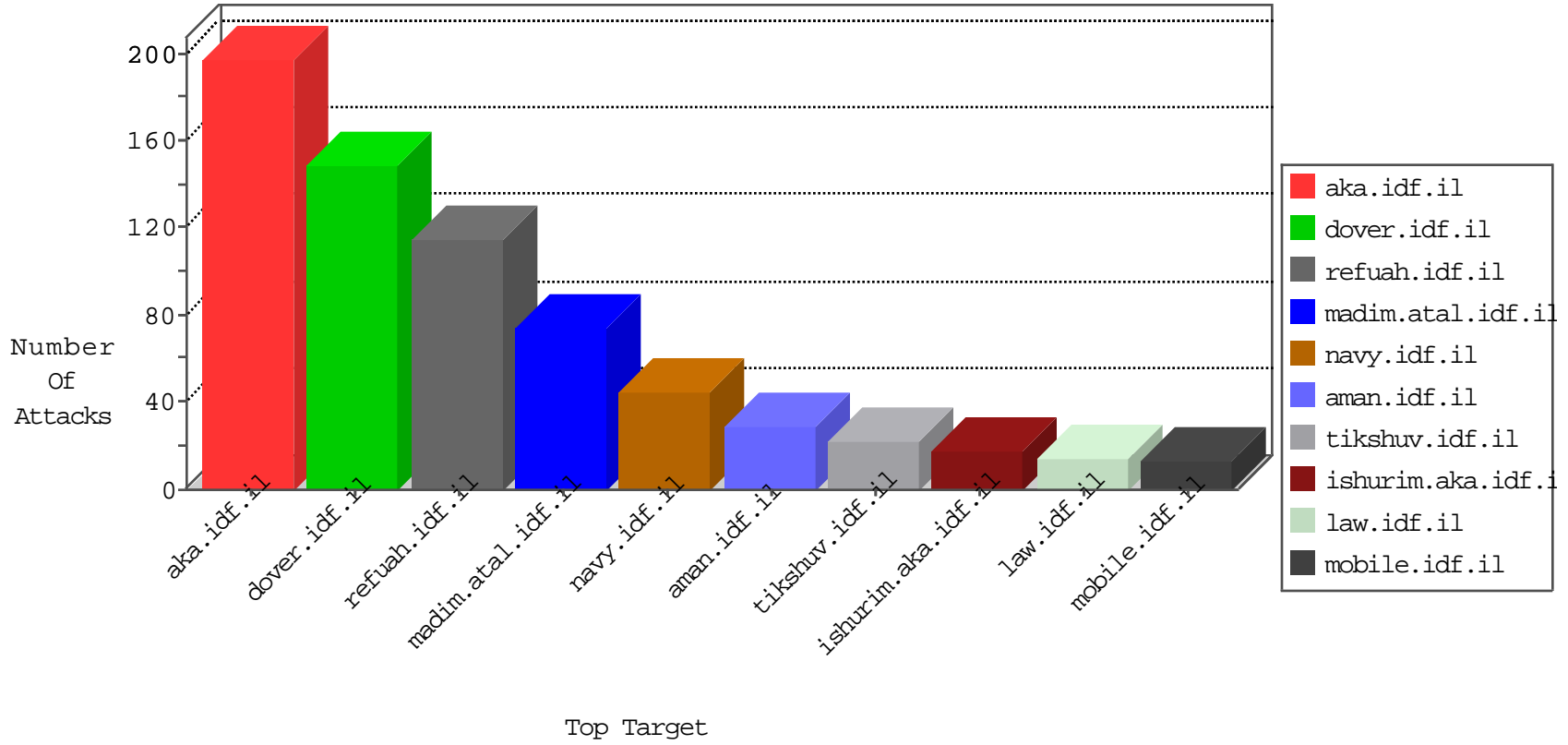


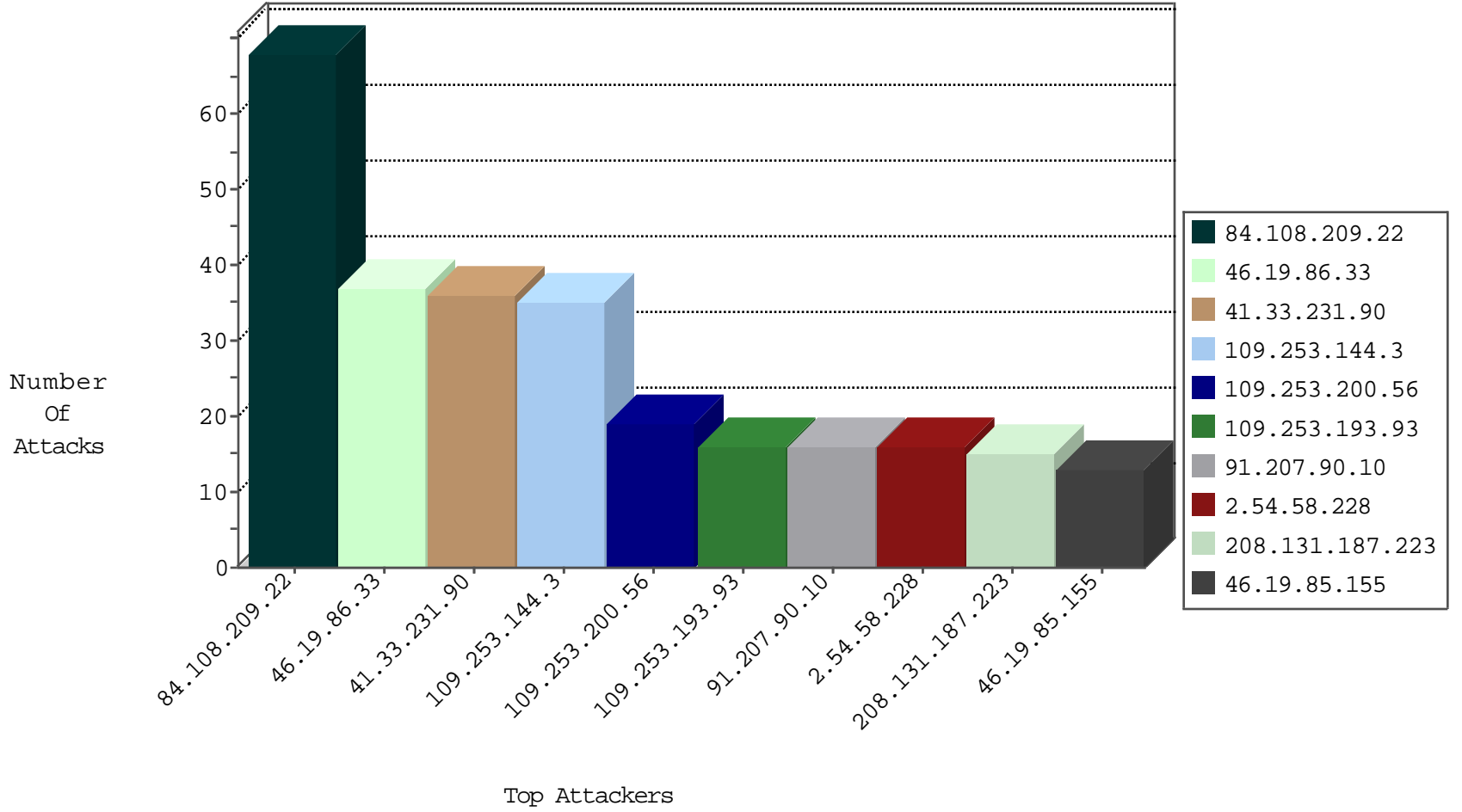
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.229.1.13	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.114	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
72.9.148.10	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.111.77	147.237.77.216	Hong Kong	dover.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.76.44	Hong Kong	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.126.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.60.36.203	147.237.8.46	United States	e.chimuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.111.77	147.237.76.199	Hong Kong	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.155.203.54	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.42	Netherlands	refuah.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
84.108.209.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.33	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
109.253.200.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
91.207.90.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.33	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.15.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.164	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.66.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.103.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.76	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.253.208.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.76	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.208.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.114.23.18	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
147.235.8.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
66.249.93.250	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.115.203.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
147.235.8.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.116.239.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.93.56	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
85.130.251.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.57.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.58.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.147.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.58.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.2.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.169.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.10.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.58.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.178.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.250	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.253.216.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.12	Israel	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
109.253.144.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.52.53.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
208.131.187.223	Jamaica	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	7
208.131.187.223	Jamaica	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.131.187.223	Block	6
2.54.172.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.163.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	3
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
188.120.154.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.120.154.65	Block	2
81.218.57.61	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.4.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	2
207.46.13.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.72	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
109.253.200.56	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.143.125.159	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct141 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.148.229	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
85.130.251.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
208.131.187.223	Jamaica	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
80.246.133.7	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
212.179.161.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
188.120.154.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
37.46.38.135	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
107.170.166.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
78.25.121.40	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.86.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
5.22.135.153	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
157.55.39.223	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
195.159.233.44	Norway	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
37.142.64.13	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
2.54.57.109	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
78.25.121.40	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
5.22.135.153	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
157.55.39.240	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
195.159.233.44	Norway	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
40.77.167.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
2.54.58.228	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.111.12	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.131.187.223	Jamaica	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/phpmoadmin/moadmin.php	Block	1
84.108.209.22	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1