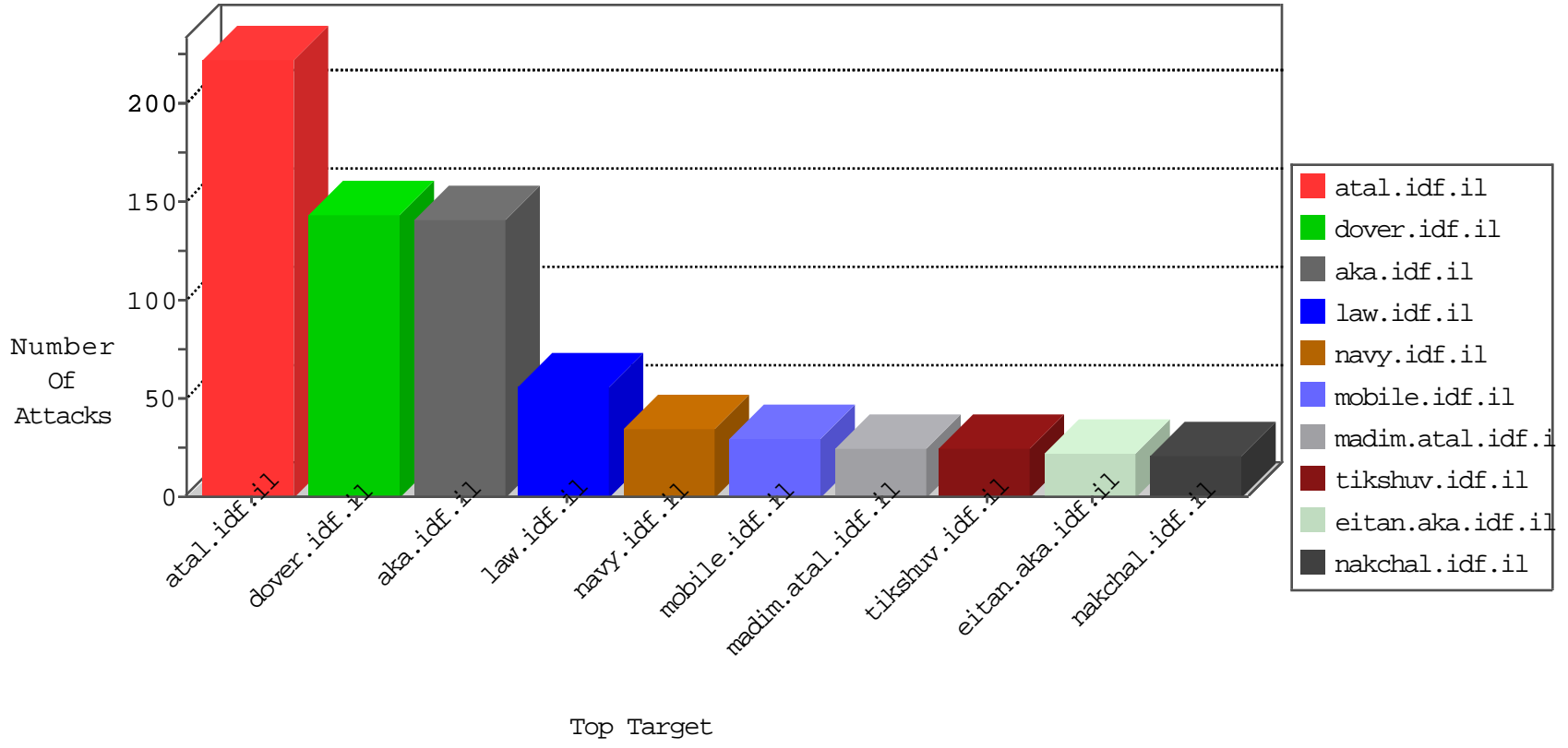


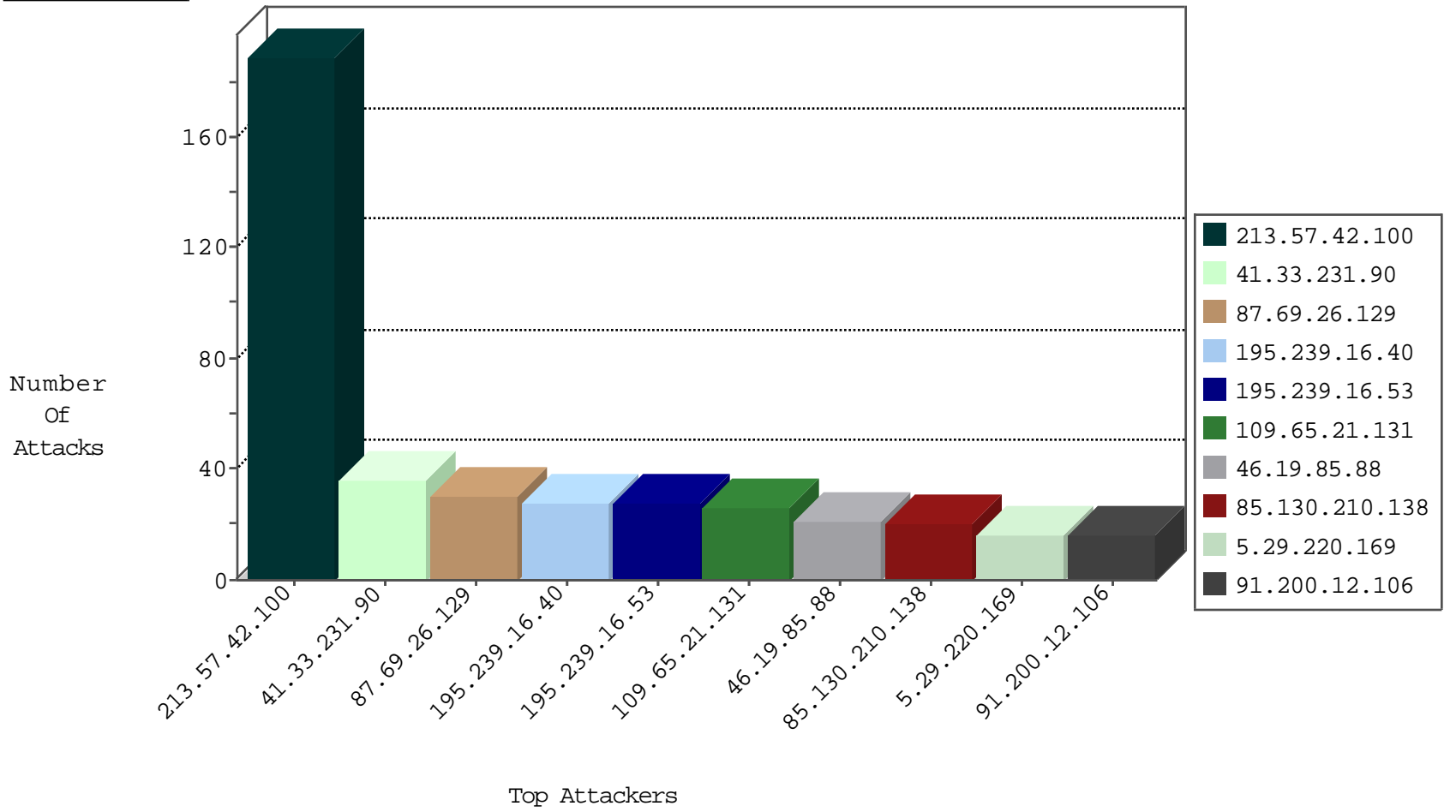
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.107.133	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
206.180.246.167	Canada	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	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	4
91.201.236.114	147.237.76.31	Ukraine	nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.2.100.21	147.237.76.38	Hungary	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
51.254.23.230	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.201.61.82	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.160	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.2.100.21	147.237.76.201	Hungary	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.201.61.82	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
123.59.53.219	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.42.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	188
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
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
109.65.21.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.85.88	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
5.29.220.169	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
87.69.26.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
89.138.31.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
74.105.32.99	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.210.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.210.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.2.185	Israel	147.237.72.166	aka.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
87.68.61.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.161.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.176.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
87.69.26.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.26.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.210.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.26.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.109.113.67	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.69.26.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.132.45.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.88	Israel	147.237.76.86	navy.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
79.182.64.67	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.178.182.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.132.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.98.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.17.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.161.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
166.170.50.56	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.192	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.181.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.170.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.254.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.179.56	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
176.13.18.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
79.177.104.60	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.23.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
178.137.17.196	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
176.13.4.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
178.137.93.235	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	2
92.195.75.88	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/german/	Block	2
185.120.126.201		147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/news/news.in.aspx	Block	1
109.65.21.131	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.111.138.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$ct113\$ct101\$ct103\$cb1Question\$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/894-he	Block	1
41.130.12.190	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.69.130.233	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.78.184	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1149-en/eitan.aspx	None	1
185.120.126.201		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp; in www.aka.idf.il/giyus/general/default.asp	None	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
87.69.130.233	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
87.69.130.233	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	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
191.101.55.60	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1764	Block	1
173.252.74.108	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
87.69.130.233	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/chinuch/klali/default.asp	None	1
213.57.42.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
46.121.238.73	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.138.31.190	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.64	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 207.46.13.64	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.65.18	Block	1
37.142.191.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
173.252.120.98	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
87.69.130.233	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/giyus/general/	None	1
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.153	Block	1
80.230.37.69	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.64	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.65.22	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1874	Block	1
41.130.12.190	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
87.69.130.233	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/982-en/eitan.aspx	None	1