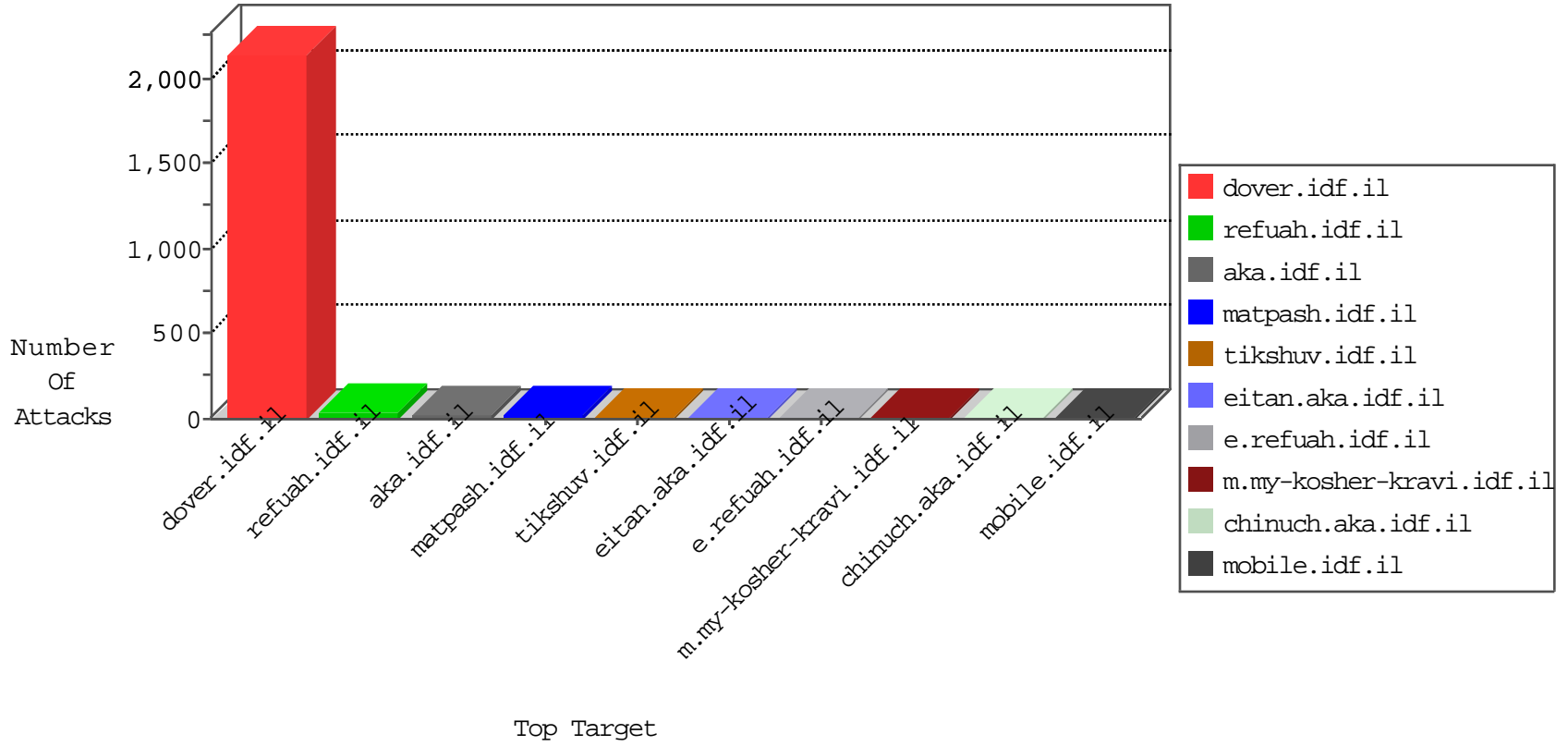


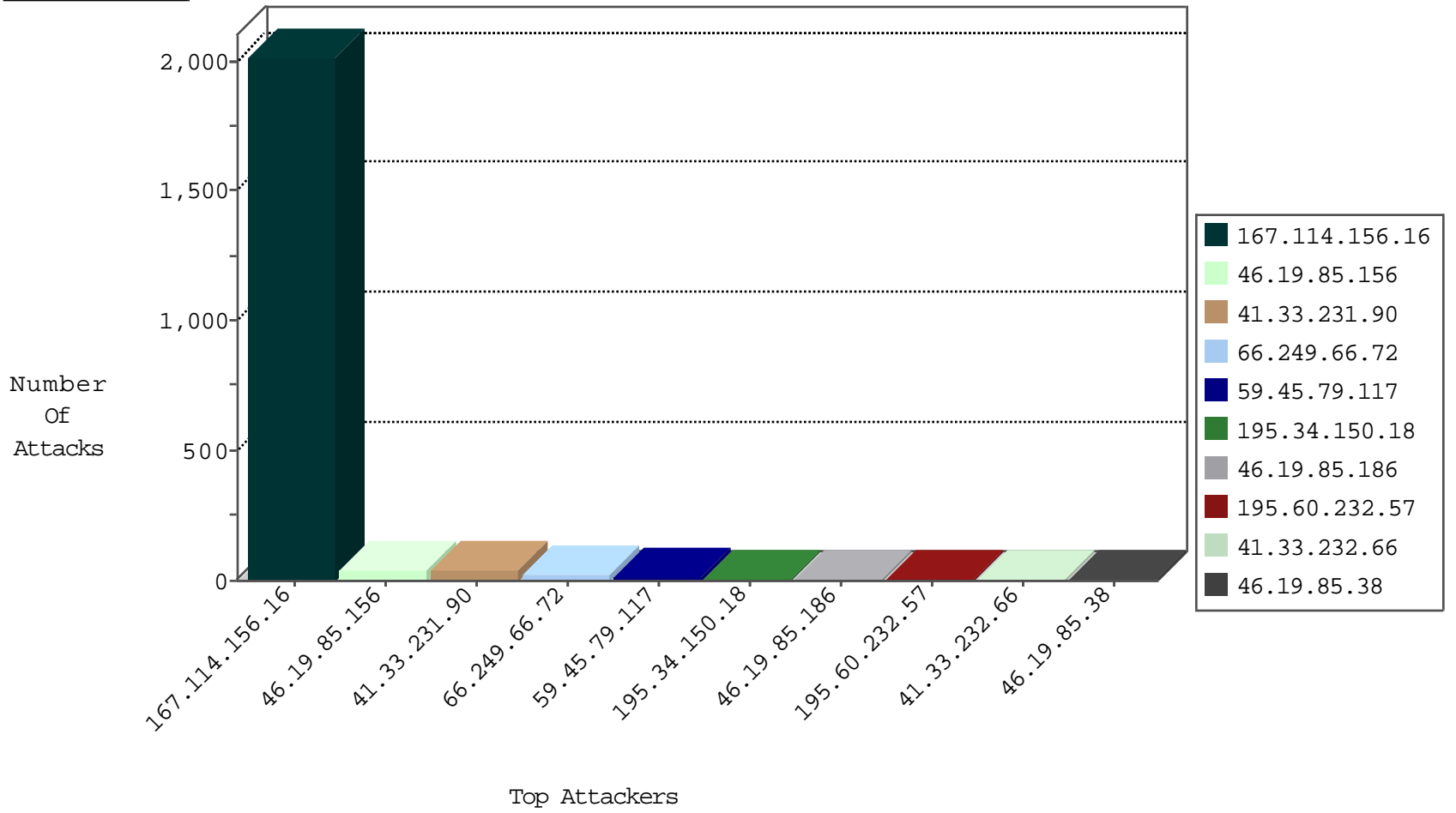
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3046
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
94.102.51.38	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.38	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.38	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.38	Netherlands	147.237.76.196	e.sviva.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
66.249.66.72	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	20
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
159.122.111.166	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
23.101.3.156	147.237.76.44	Hong Kong	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.169.86	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
108.168.185.133	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.169.86	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
23.101.3.156	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.135.131	147.237.0.35	United States	akaws.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.30.25.105	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.234.170.169	Sweden	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
108.44.233.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
149.210.150.83	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
198.20.69.74	United States	147.237.8.46	e.chimuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.153.5.236	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.228	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
173.14.173.227	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.255.253.74	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
109.201.133.100	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
50.253.127.139	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.94	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.8.109.19	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.153.5.236	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.251	United States	147.237.0.33	idf.il	drop		drop	1
176.31.121.196	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.255.253.74	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
128.52.128.105	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.72	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
61.135.190.71	China	147.237.0.33	idf.il	drop		drop	1
184.105.139.98	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.122.111.166	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
204.17.56.42	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.30	United States	147.237.8.46	e.chimuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
24.218.80.94	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
218.22.211.69	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.114	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/Ã¸Ã¸ Ã¸Ã¸ "Ã¸Ã¸,Ã¸?	Block	1
104.128.144.131	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/jquery/jquery-1.9.1.js	Block	1
190.162.174.52	Chile	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
91.226.14.124	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
40.77.167.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/faq.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
61.135.190.197	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
91.226.14.124	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1399-en/dover.aspx	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/information.aspx	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/text.css	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.78.159	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/960.css	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.226.14.124	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1399-en/dover.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19771-he/idfgdover.aspx	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
73.153.5.236	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
91.226.212.39	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
61.135.190.72	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
180.76.15.21	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.109.139.87	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout.css	Block	1