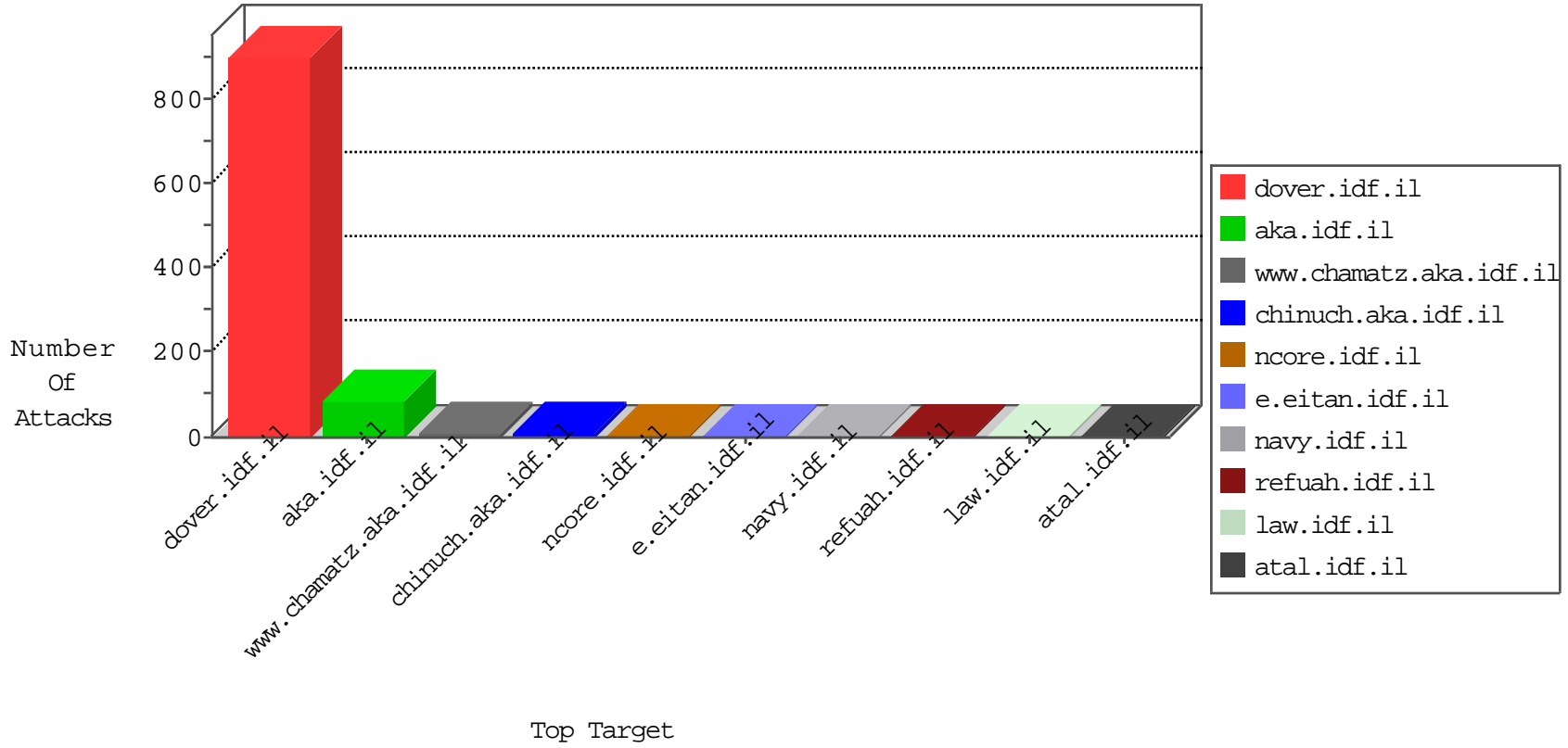


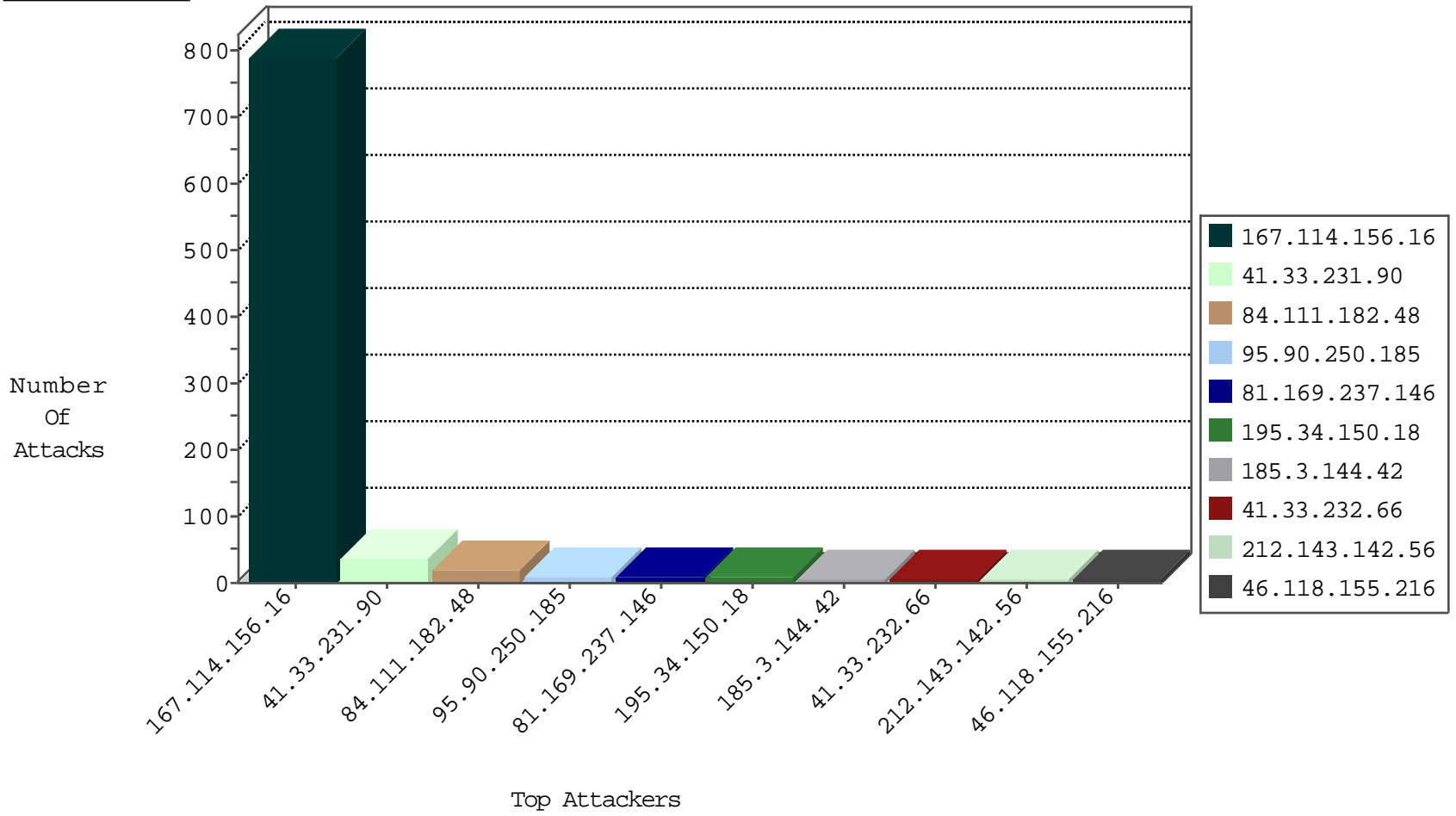
IDF Under Attack Daily Report



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	3007
89.248.174.4	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
65.181.113.88	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

01-10-2016-02:04:02 to 01-10-2016-03:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.97.23	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	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
193.104.41.54	147.237.76.177	Moldova, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
175.150.131.81	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
31.211.102.129	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
183.82.106.200	147.237.76.202	India	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 3072	1
58.45.134.223	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.196	147.237.77.243	Netherlands	mobile.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	34
95.90.250.185	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
84.111.182.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
84.111.182.48	Israel	147.237.72.166	aka.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	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.179.160	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
100.36.168.5	United States	147.237.72.166	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
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.169.237.146	Germany	147.237.76.177	noore.idf.il	drop	SAM rule	drop	4
99.98.124.202	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
62.219.138.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.78.9	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	SYN Attack		reject	2
118.193.222.243	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
61.242.114.152	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.235		147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
71.183.108.102	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
45.49.178.22		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.3.147.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.21.147	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.142.64.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
71.183.108.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
45.49.178.22		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.22.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
37.142.64.45	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.216.46.75	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.183.108.102	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
46.19.85.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.235		147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
2.54.25.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.235		147.237.76.176	test.noore.idf.il	drop	SAM rule	drop	1
2.54.25.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	3
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
80.246.136.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	2
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	2
84.111.182.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
75.119.200.140	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 75.119.200.140	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/klali/default.aspx?catid=42858&docid=45780	Block	1
80.178.17.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58606	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2293.jpg	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.105.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=65415	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
185.72.178.65		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
109.66.191.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.136	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/css/jquery.kxslider.css.jsp	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
87.69.107.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteyerua	Block	1
185.130.5.214		147.237.77.216	dover.idf.il	PHP Attempt	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
109.201.138.237	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
80.246.136.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/hovot/templates/main.asp	Block	1
150.70.173.40	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.126.26.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59269	Block	1
185.130.5.214		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
212.76.98.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
109.201.152.3	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59391&docid=65366	Block	1
150.70.173.53	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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