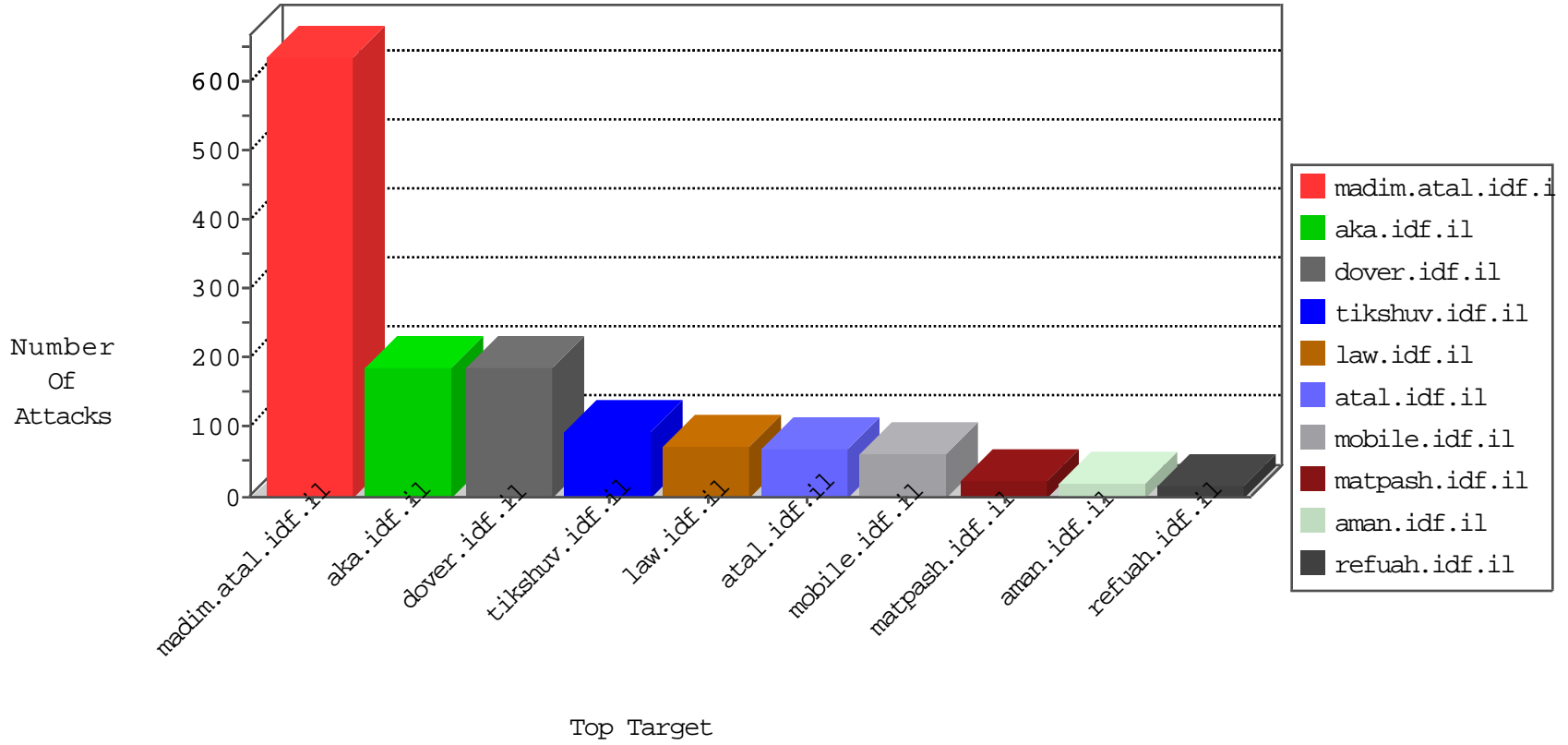


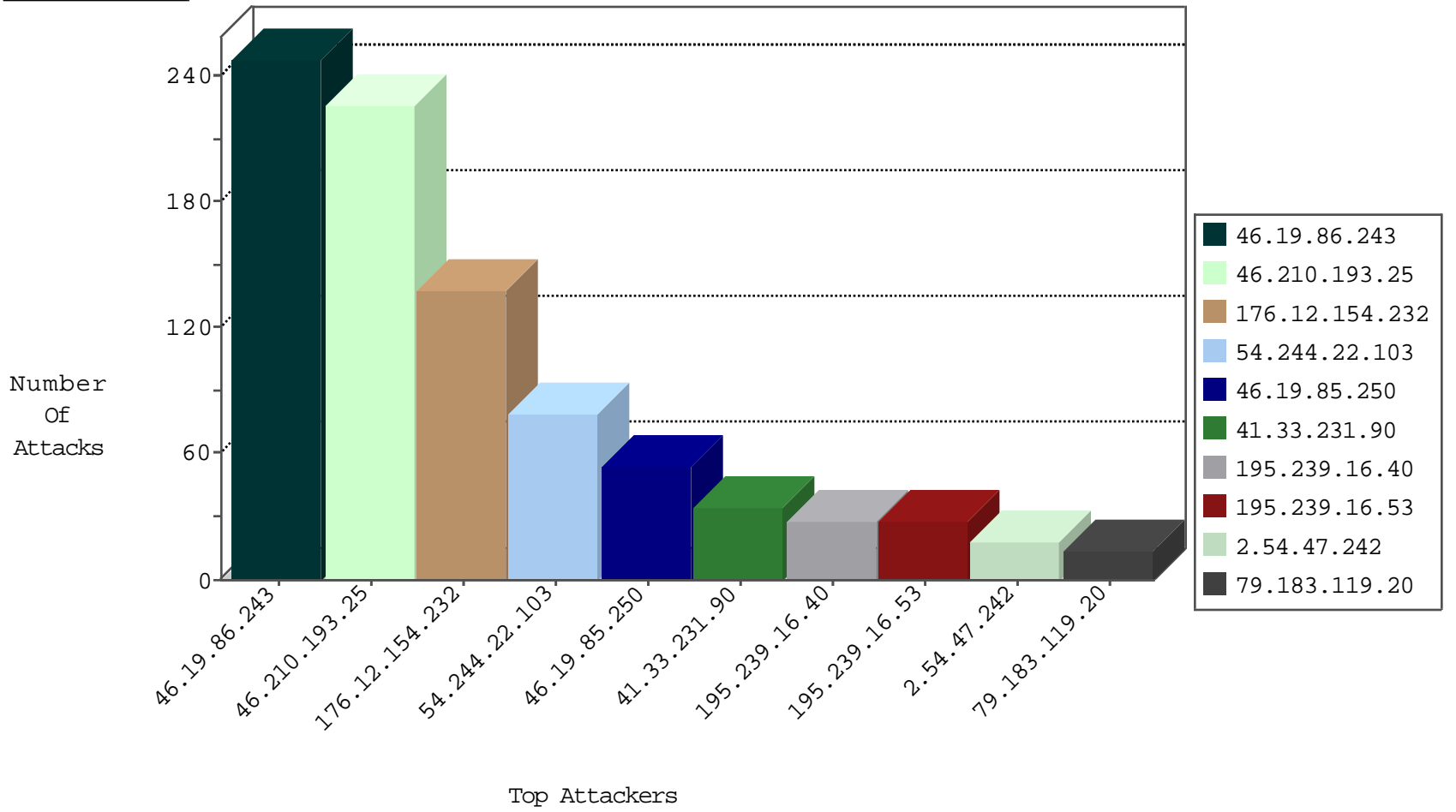
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
142.54.169.162	United States	147.237.72.156	anan.idf.il	block-sp-trafl	drop	1
198.27.79.227	Canada	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.210	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-trafl	forward	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
85.136.227.77	Spain	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
94.102.153.58	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	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
85.136.227.77	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	3
94.102.153.58	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	3
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	3
66.249.66.72	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.139	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
117.41.184.227	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.193.160.43	147.237.77.19	China	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.66	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
145.255.2.133	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
145.255.2.133	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
117.41.184.227	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
145.255.2.133	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	69
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.250	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
141.0.15.36	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
77.126.168.115	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.47.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.155.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.248.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.204.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.98.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.183.119.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.68.153.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.8.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.119.20	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.18.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
82.145.218.95	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.188.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
187.147.252.133	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.109.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.186.28	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
189.218.244.31	Mexico	147.237.0.200	mAu.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
185.3.147.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.230.86.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.58.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.2.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.43.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.218.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.147.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.235	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.22.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.167.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.114.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.236.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.235	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.193.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	174
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	140
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
176.12.154.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
176.12.154.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
46.210.193.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
80.246.130.246	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
176.12.154.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.173	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.173	Block	7
46.19.85.173	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	5
79.177.61.49	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
31.210.186.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935-4489-he/patzar.asp	Block	3
149.78.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.47.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.64.50.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.76	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 80.246.130.76	Block	3
176.12.155.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
17.138.59.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	2
197.38.205.132	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
80.178.102.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.155.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.28.137.35	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	2
5.102.246.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.38.205.132	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	1
176.103.54.50	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
142.54.160.210	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.xy9.com/	Block	1
85.64.215.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.38.146	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
98.143.148.107	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/check	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding â,~?Ã"z\,•#Ã [[#2]]pw%Ã! .3Ö²Ã™ ÖuÃwâ?â,çâ,çÃ-Ã s	Block	1
84.94.73.136	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/3/1723.pdf	Block	1
191.232.136.19	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
87.68.18.221	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
212.76.113.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
79.177.61.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
46.19.86.35	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
99.1.240.226	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Malformed URL â,~?Ã"z\,•#Ã [[#2]]pw%Ã! .3Ö²Ã™ ÖuÃwâ?â,çâ,çÃ-Ã s	Block	1
84.228.163.176	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
191.232.136.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
162.194.18.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.147.33.61	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
93.223.139.140	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
109.66.229.4	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/gyus/general.aspx	None	1
192.241.141.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1