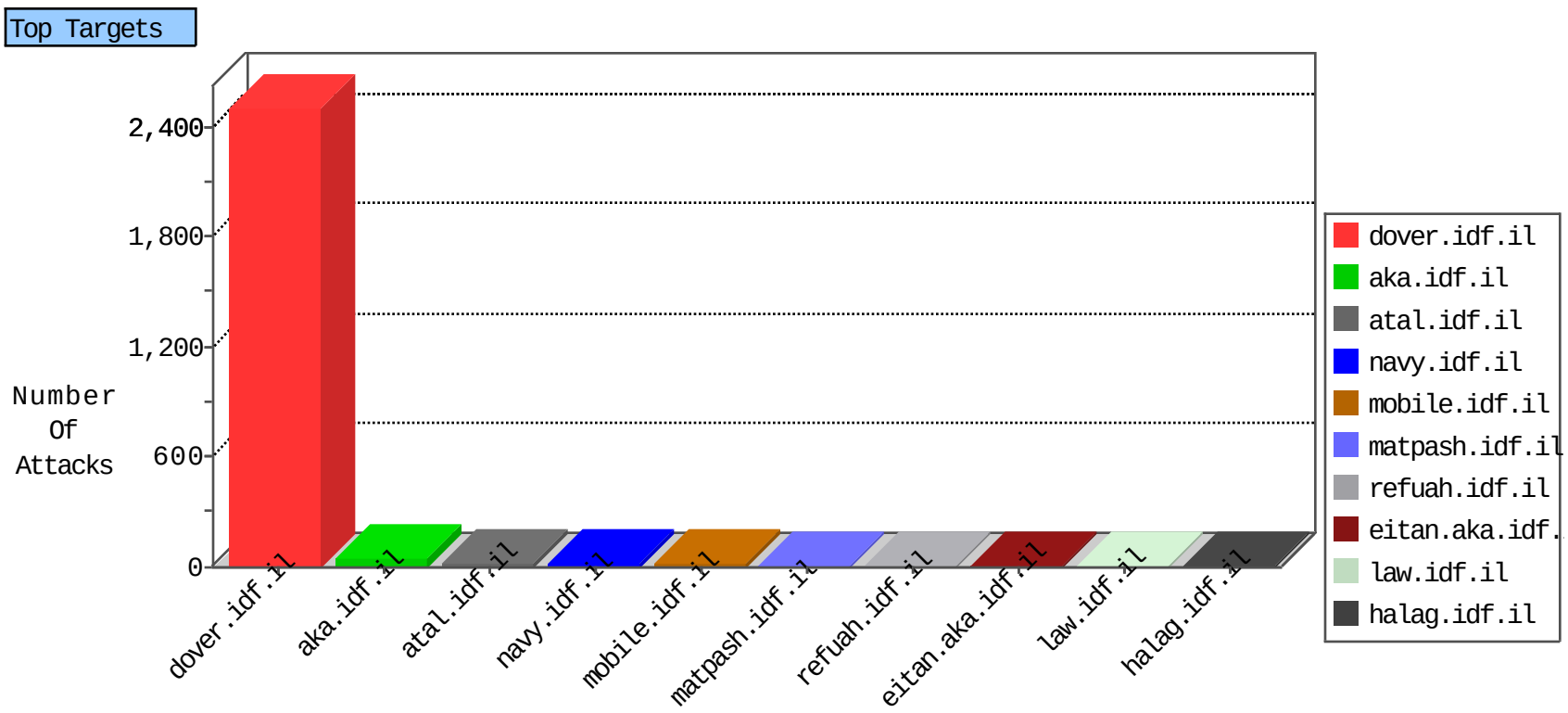
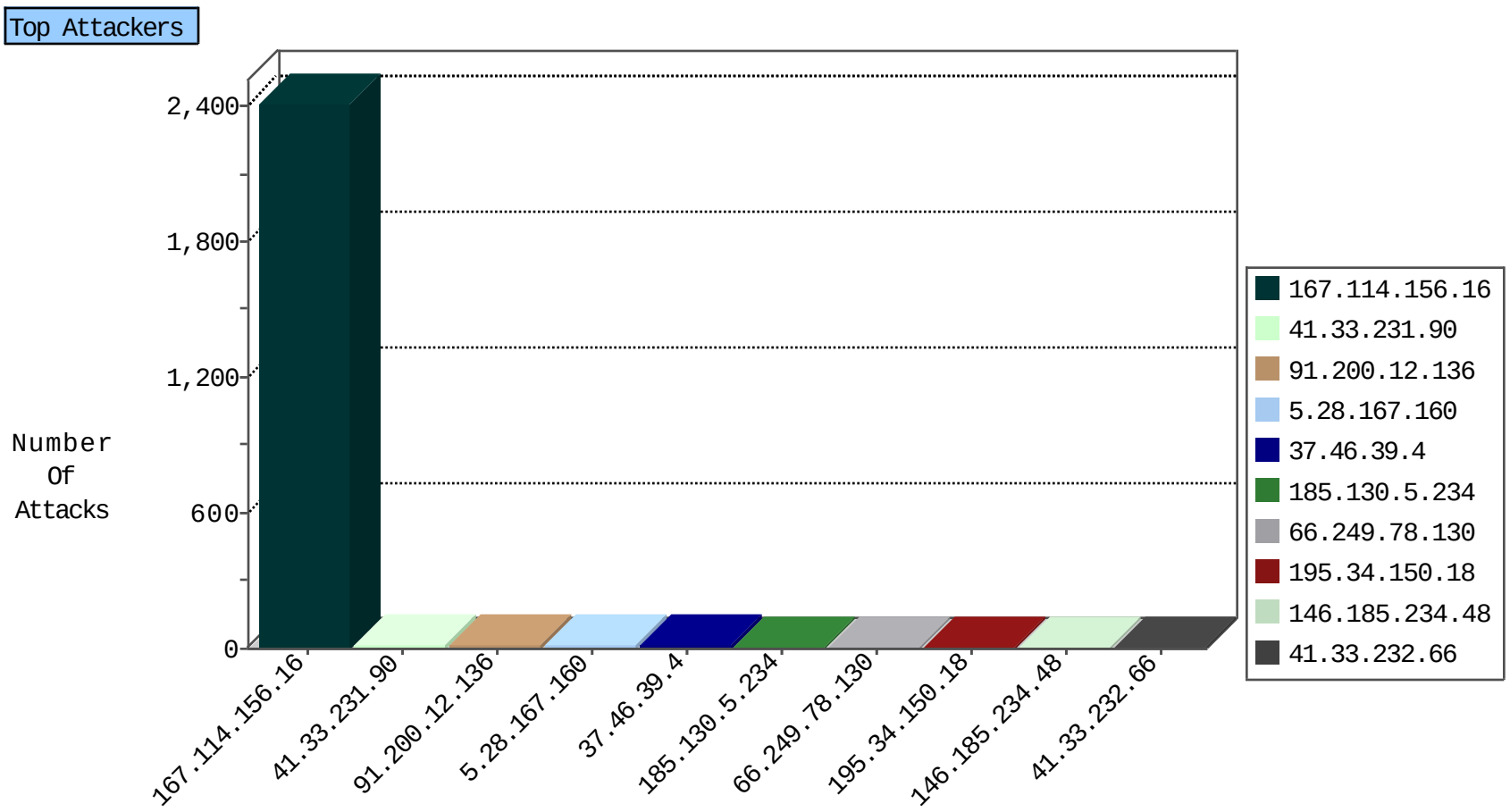
01-24-2016-02:04:08 to 01-24-2016-03:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-24-2016-02:04:08 to 01-24-2016-03:04:08

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	3055
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	878
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
113.171.23.126	Vietnam	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.160.138	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

01-24-2016-02:04:08 to 01-24-2016-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.153	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-24-2016-02:04:08 to 01-24-2016-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.234	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.234	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
137.117.168.203	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
42.119.247.121	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.227.181	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.234	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
42.119.247.121	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
212.179.227.181	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
23.101.3.156	147.237.0.33	Hong Kong	idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.234	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1

01-24-2016-02:04:08 to 01-24-2016-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.28.167.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
37.46.39.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
149.78.253.3	Israel	147.237.76.200	eitan.aka.idf.i	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
133.130.49.166	Japan	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
91.200.12.136	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.221.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.146.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
163.53.176.91	India	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
8.25.157.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.46.39.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.121.192	United States	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	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
23.27.220.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
185.3.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.106	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
84.108.39.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
207.46.13.140	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
71.9.171.235	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.185.4.15	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
123.125.71.106	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.39.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.241.237.240	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.222	Israel	147.237.76.31	nakchal.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
186.202.151.18	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.151.18	Block	3
95.32.13.152	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/configuration.php_	Block	2
5.28.167.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.127.57.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.76.101.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.63.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
213.57.151.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/s	Block	1
186.202.151.18	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
204.45.207.58	United States	147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
157.55.39.52	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1236-he/atal.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
204.13.201.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.173.43	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.150.45.106	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.90	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
37.46.39.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
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	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
150.70.173.43	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.150.45.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	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
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.209.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.5	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1402-he/atal.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
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-11039-he/dover.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
84.109.212.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.45.207.58	United States	147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
157.55.39.51	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1368-he/atal.aspx	Block	1