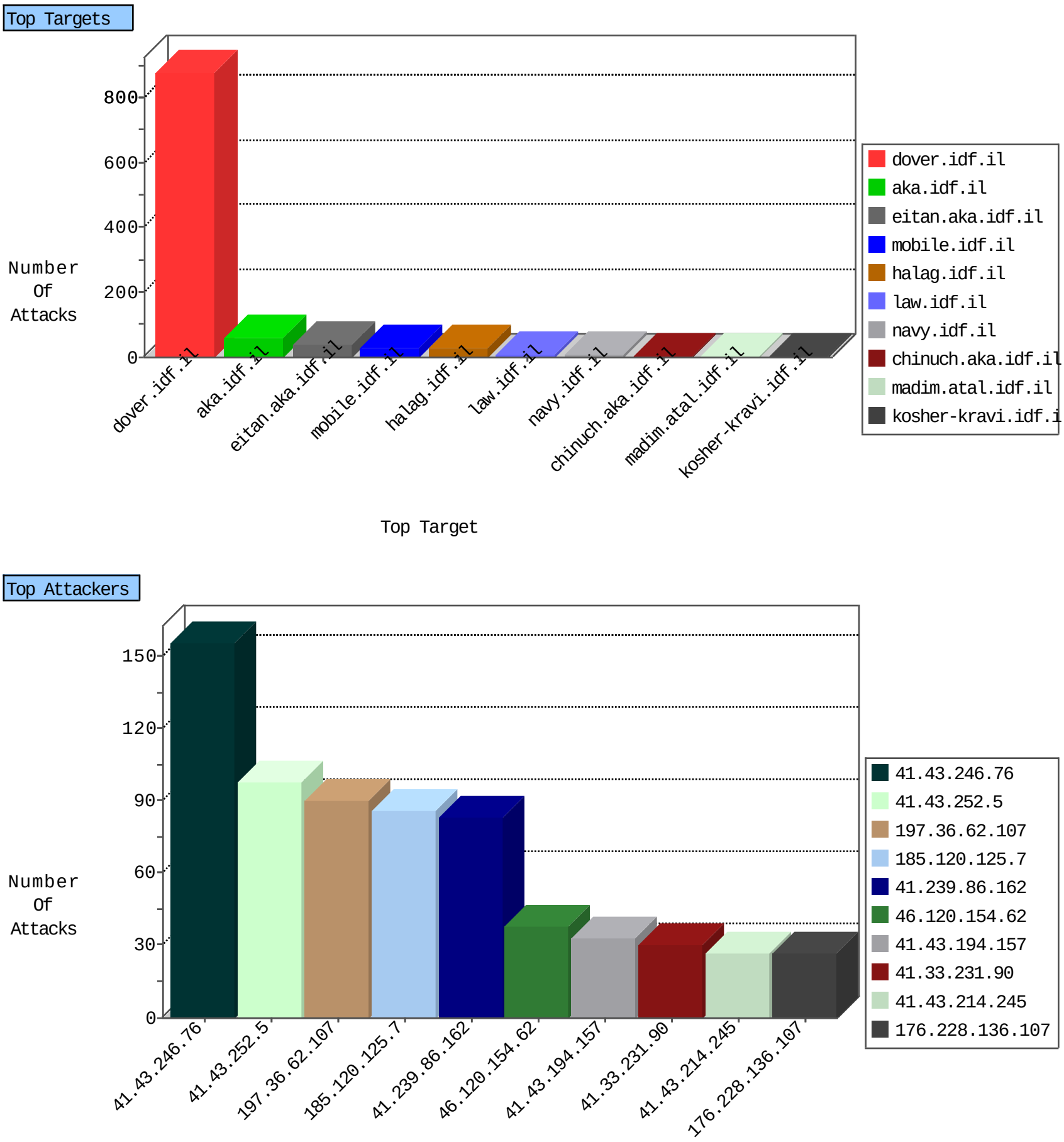
02-01-2016-02:04:06 to 02-01-2016-03:04:06

IDF Under Attack Daily Report



02-01-2016-02:04:06 to 02-01-2016-03:04:06

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	837
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	731
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	38
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	34
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	19
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	18
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	17
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	12
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	11
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	9
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5
41.43.194.157	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
41.47.56.154	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	3
52.53.253.180	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
92.223.198.233	Italy	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	2
41.239.83.147	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.239.228.10	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
52.53.253.180	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
74.91.28.61	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
41.43.194.157	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
197.41.137.4	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
41.239.83.147	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
41.42.108.85	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
41.42.108.85	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1

02-01-2016-02:04:06 to 02-01-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-01-2016-02:04:06 to 02-01-2016-03:04:06

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
50.204.188.142	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
41.239.86.162	147.237.77.216	Egypt	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	1
41.47.56.154	147.237.77.216	Egypt	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	1
197.36.62.107	147.237.77.216	Egypt	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	1
41.43.252.5	147.237.77.216	Egypt	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
41.43.194.157	147.237.77.216	Egypt	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	1
173.55.32.113	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
146.0.75.114	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.146	147.237.76.177	Vietnam	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
41.239.86.162	147.237.77.216	Egypt	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	1
41.47.56.154	147.237.77.216	Egypt	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	1
197.36.62.107	147.237.77.216	Egypt	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	1
41.43.252.5	147.237.77.216	Egypt	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	1
41.43.194.157	147.237.77.216	Egypt	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
27.124.121.194	147.237.76.42	Australia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
158.130.6.191	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
146.0.75.114	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.53.101.68	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-01-2016-02:04:06 to 02-01-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.120.154.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
176.228.136.107	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
41.43.194.157	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.42.108.85	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.28.163.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.43.208.21	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.239.83.147	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.43.251.49	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.47.56.154	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.20.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.218.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.43.246.76	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	4
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.43.251.49	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
197.41.137.4	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.36.62.107	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	4
41.43.252.5	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	4
197.41.224.3	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.23.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.239.86.162	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	3
37.46.38.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
41.43.214.245	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	3
197.41.224.3	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
41.239.83.147	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
41.42.108.85	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
41.43.208.21	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
41.43.241.123	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
197.41.137.4	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
41.47.56.154	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
41.42.108.102	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2
46.19.86.130	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
41.43.194.157	Egypt	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	DirBuster Security Scanner	reject	2

02-01-2016-02:04:06 to 02-01-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.218.0	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	6
65.49.17.2	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 65.49.17.2	Block	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.218.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
202.123.131.18	Guam	147.237.77.74	law.idf.il	PHP Attempt	Block	2
104.223.39.109	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.20.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
202.123.131.18	Guam	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
42.101.158.20	China	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/plus/mytag_js.php	Block	1
150.70.173.57	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.214.98.239	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.23.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1134-7935-he/dover.aspx	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
89.139.36.122	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
65.49.17.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
40.77.167.22	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx)	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.228.136.107	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
96.255.136.28	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	1
40.77.167.35	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/0/2540.jpg	Block	1
79.179.58.201	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.131	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/0/1350.pdf	Block	1
42.101.158.20	China	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	1
150.70.173.57	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.111.114.7	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.120.164.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

02-01-2016-02:04:06 to 02-01-2016-03:04:06