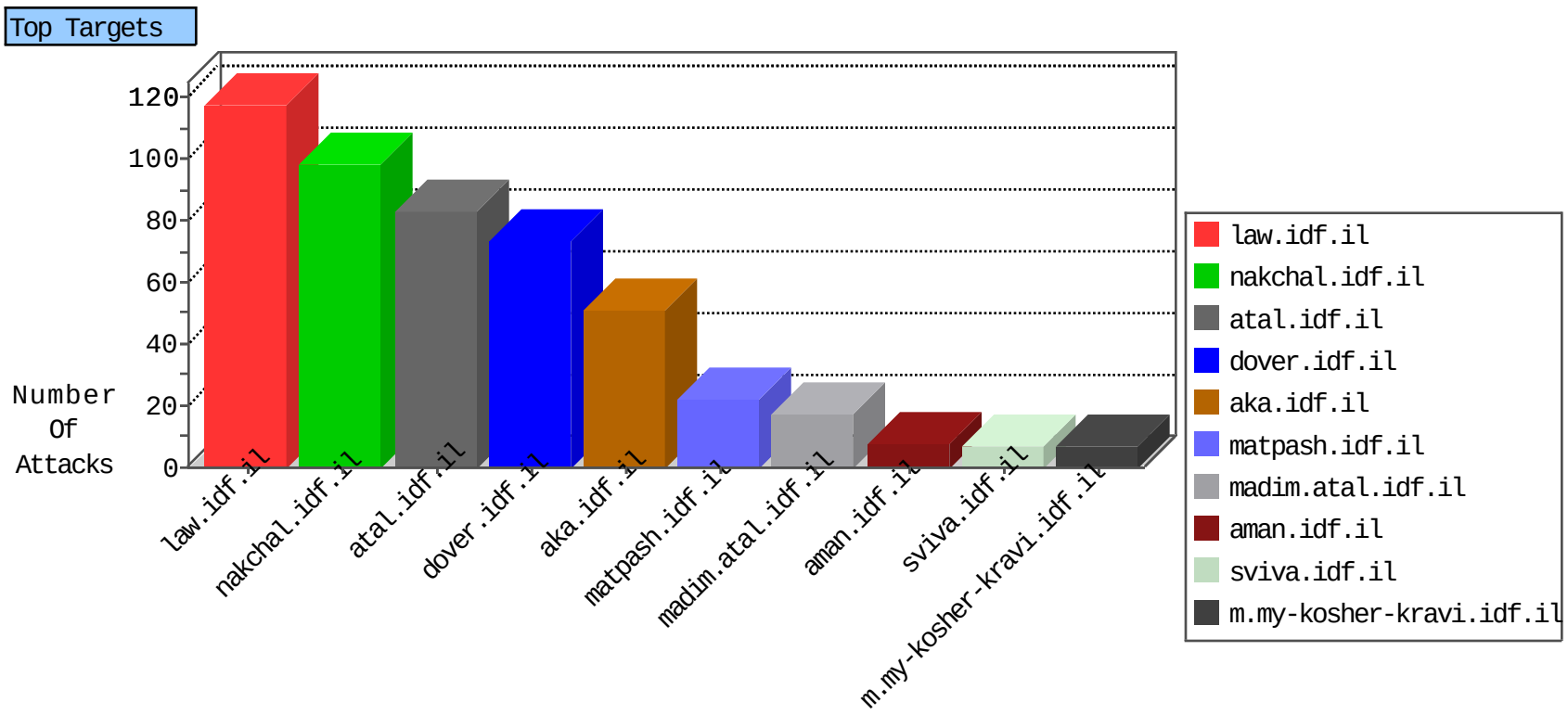
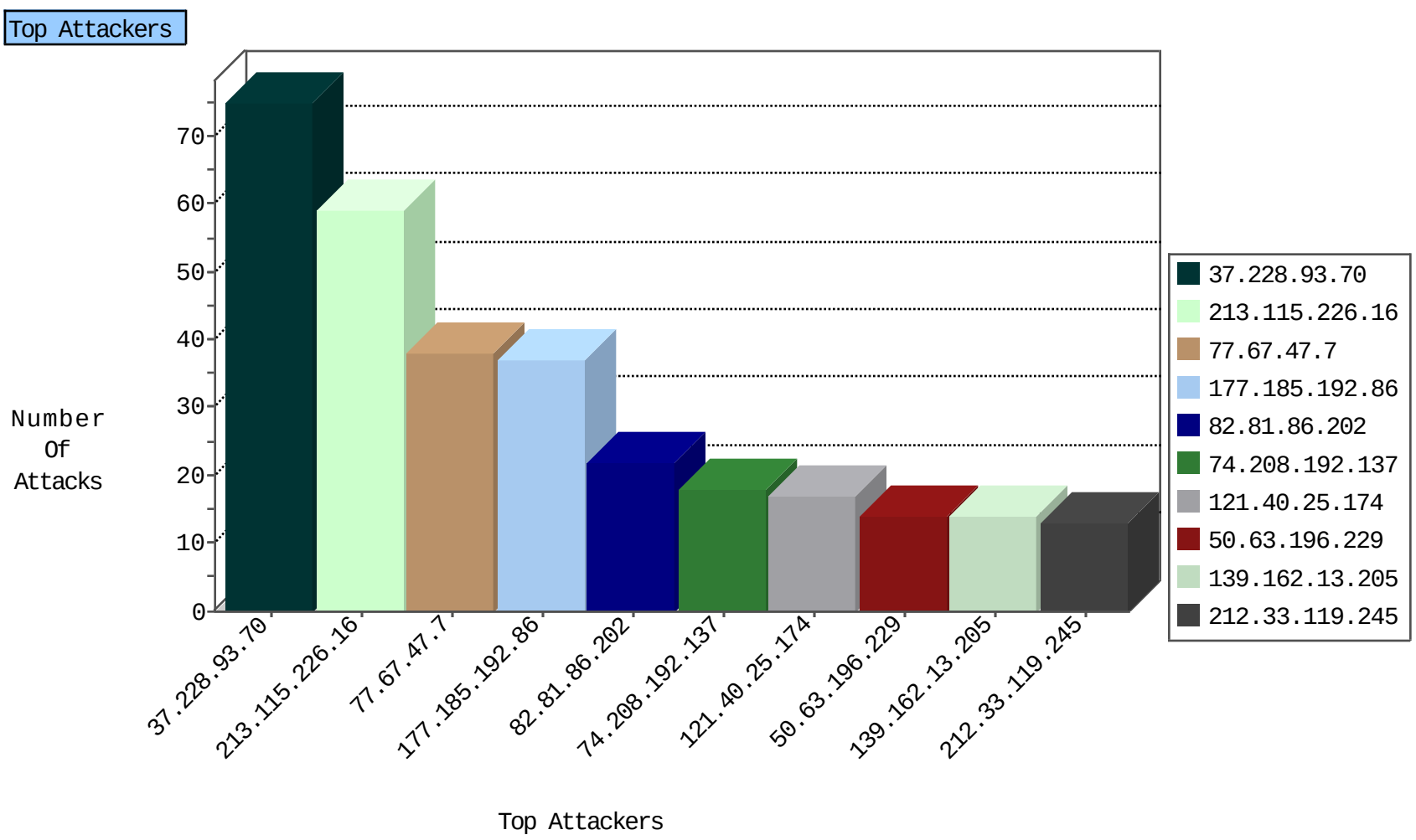
08-24-2016-16:04:00 to 08-24-2016-17:04:00

IDF Under Attack
Daily Report





08-24-2016-16:04:00 to 08-24-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.84.0.150	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
212.25.74.130	Israel	147.237.77.233	atal.idf.il	Black List	drop	1

08-24-2016-16:04:00 to 08-24-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.67.47.7	France	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
213.115.226.16	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
37.228.93.70	Russian Federation	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
177.185.192.86	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
77.67.47.7	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
37.228.93.70	Russian Federation	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.229	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.173	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
121.40.25.174	China	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
31.31.73.93	Czech Republic	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
31.31.73.93	Czech Republic	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
121.40.25.174	China	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	2

08-24-2016-16:04:00 to 08-24-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.228.93.70	147.237.76.31	Russian Federation	nakchal.idf.il	SQL Injection - Select From	60
213.115.226.16	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	48
177.185.192.86	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	29
77.67.47.7	147.237.77.74	France	law.idf.il	SQL Injection - Select From	20
121.40.25.174	147.237.77.233	China	atal.idf.il	SQL Injection - Select From	12
50.63.196.229	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
216.119.125.173	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
205.144.171.34	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
77.124.247.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
202.112.38.190	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
82.81.46.240	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	1
79.177.119.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.3.168	147.237.77.216	Japan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
108.29.44.222	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
84.229.43.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.217.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.102	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.57.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.101.36	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
185.69.145.175	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.189.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.146.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-24-2016-16:04:00 to 08-24-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.208.192.137	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
212.33.119.245	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
139.162.13.205	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	7
139.162.13.205	Singapore	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	7
100.92.249.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
87.68.7.3	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	6
185.120.125.111	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.243.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.12.160.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.16.75.149	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
31.223.176.126	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.241.162	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
83.110.105.76	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
85.114.113.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.144.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
95.90.210.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.225.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
134.35.162.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.120.125.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.8.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.134.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.243.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.16.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.243.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
176.13.18.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.40.0.13	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.248.203	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.147	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
129.56.2.38	Nigeria	147.237.76.34	yohalan.idf.il	drop		drop	1
77.40.0.13	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-24-2016-16:04:00 to 08-24-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.86.202	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	12
82.81.86.202	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 82.81.86.202	Block	9
212.29.210.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
65.49.68.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
95.35.161.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.212.17.139	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
89.237.117.47	France	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/206-he/patzar.aspx	Block	2
185.27.105.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.237.117.47	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	2
2.53.160.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
193.222.81.163	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
82.81.86.202	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.139.227.46	France	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/favicon.ico	Block	1
62.0.60.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
150.70.173.54	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
87.69.105.76	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.168.220.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
79.183.52.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/hermon.aspx	Block	1
109.64.18.47	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
85.114.113.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.177.2.96	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
157.55.39.122	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
89.139.191.118	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
31.223.176.126	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
80.179.20.132	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
213.8.245.193	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
199.30.25.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal	Block	1
109.64.18.47	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
85.114.113.79	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.179.141.50	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.102.9.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
37.26.146.137	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 37.26.146.137	Block	1
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
204.79.180.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
77.124.54.23	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.64.145.133	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.37.146	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.180.79.142	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
212.179.242.199	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1

08-24-2016-16:04:00 to 08-24-2016-17:04:00