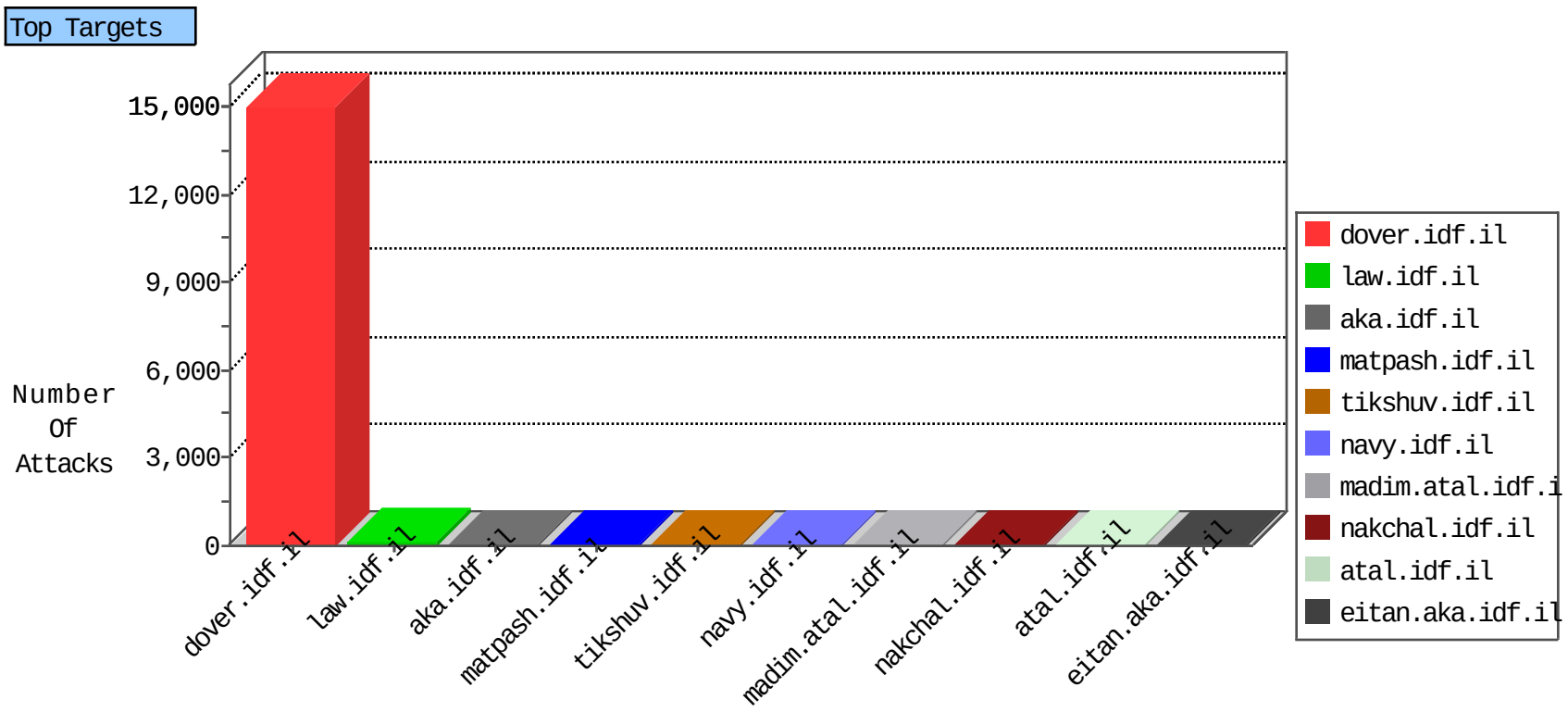
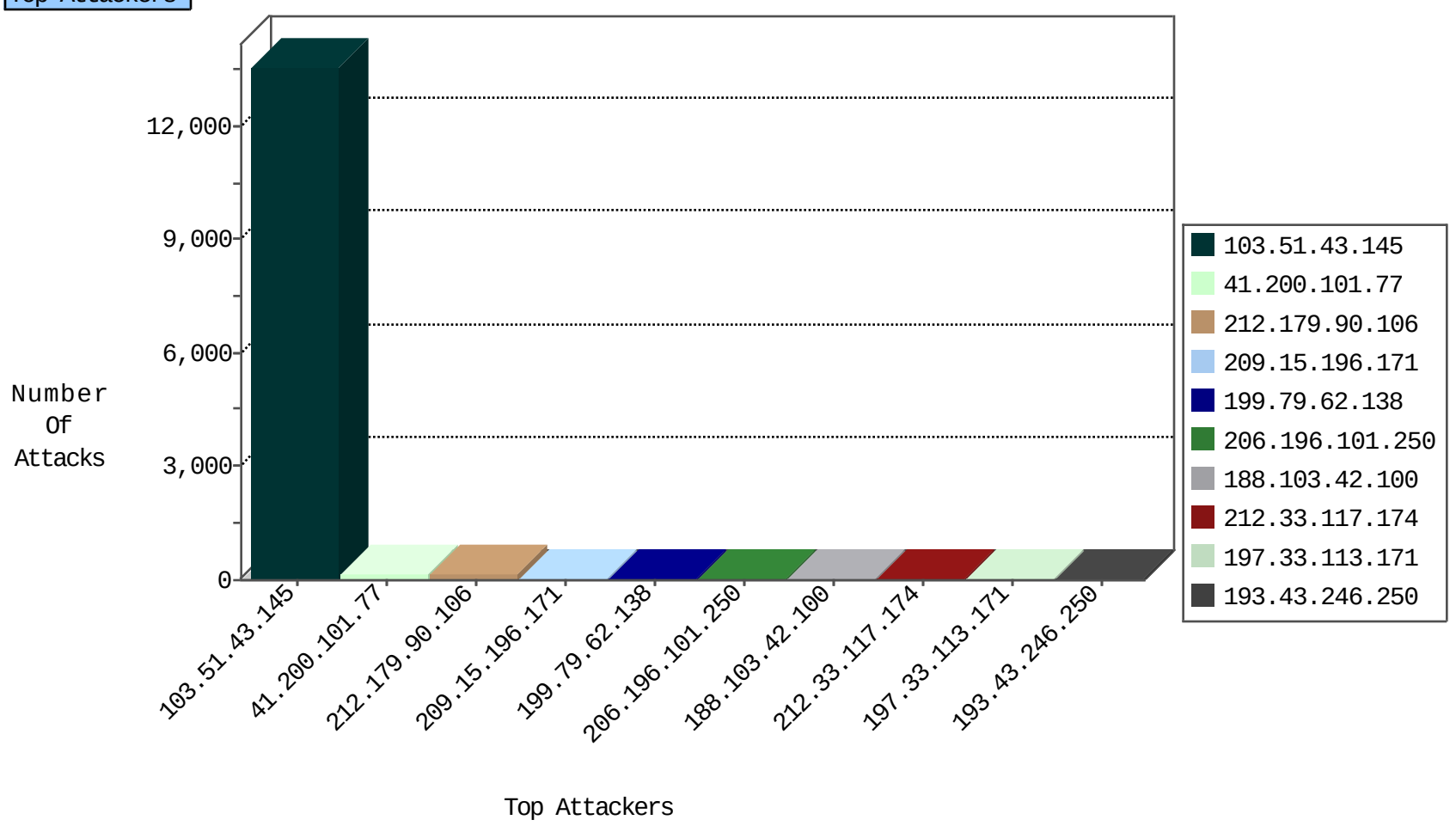
08-22-2016-21:04:02 to 08-22-2016-22:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-22-2016-21:04:02 to 08-22-2016-22:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
103.51.43.145	Malaysia	147.237.77.216	dover.idf.il	HTTP-MISC-DosTool-SlowPOST	dest-reset	13202
8.37.231.87	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	8
77.125.0.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.121.52.2	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
80.82.77.38	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
80.82.77.38	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
71.6.146.185	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1

08-22-2016-21:04:02 to 08-22-2016-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.171	Canada	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
199.79.62.138	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.144.249.54	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
199.79.62.138	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.15.196.171	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
174.47.99.30	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
206.196.101.250	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
83.168.250.50	Sweden	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
206.196.101.250	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.46.19	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.171	Canada	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.121.86.136	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
50.63.197.145	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
168.144.249.54	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-22-2016-21:04:02 to 08-22-2016-22:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
206.196.101.250	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	36
199.79.62.138	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	36
209.15.196.171	147.237.0.34	Canada	tikshuv.idf.il	SQL Injection - Select From	20
184.168.27.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
168.144.249.54	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
83.168.250.50	147.237.72.166	Sweden	aka.idf.il	SQL Injection - Select From	8
209.15.196.171	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	8
184.168.46.19	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
174.47.99.30	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
168.144.249.54	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	6
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
50.63.197.145	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
66.240.213.93	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.100.214.202	147.237.76.177	Australia	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
59.100.214.202	147.237.76.177	Australia	ncore.idf.il	ET SCAN NMAP -f -sS	1
163.172.66.234	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
8.37.231.87	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
161.10.5.40	147.237.0.19	Colombia	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.123.119.180	147.237.72.167	China	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
213.202.233.62	147.237.72.167	Germany	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
80.246.137.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.100.214.202	147.237.76.177	Australia	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
123.206.85.139	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
110.35.218.167	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.156.215.30	147.237.76.177	Turkey	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.246.138.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.14.153	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

08-22-2016-21:04:02 to 08-22-2016-22:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
103.51.43.145	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13071
41.200.101.77	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	166
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
188.103.42.100	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	35
212.33.117.174	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
193.43.246.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	21
5.102.254.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
197.33.113.171	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.228.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.79.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.120.148.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.205.61.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.70.9.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.10.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
131.253.27.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.119.73.60	Saudi Arabia	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.120.130.2	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	drop	First packet isn't SYN	drop	6
77.125.61.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
197.14.53.58	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.67.29.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.161.52.239	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
5.102.195.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.200.148.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.168.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.241.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.181.225.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.116.189.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.65.143.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.8.111.193	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.34.167.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.253.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.158.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.71.43.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.161.52.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.225.204.41	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.55.129.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.226.232	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.230.228.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

08-22-2016-21:04:02 to 08-22-2016-22:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.9.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
213.57.55.170	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	10
197.33.113.171	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.33.113.171	Block	8
84.94.61.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.94.61.63	Block	5
213.57.55.170	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 213.57.55.170	Block	5
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
85.65.79.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.79.82	Block	4
213.57.55.170	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
87.120.142.33	Bulgaria	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.49.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	3
109.253.136.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
81.18.201.4	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
213.57.42.200	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.191.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
197.15.213.8	Tunisia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
89.138.18.24	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
46.19.86.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.30.134	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
94.230.86.43	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	2
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
46.19.86.11	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/הטענת טלפון דיגסגוף modiin/kiosk.aspx	Block	1
141.255.42.69	Greece	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 141.255.42.69	Block	1
5.29.193.198	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
77.139.206.66	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
197.33.113.171	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23228-ar/	Block	1
109.64.45.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.8.29	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.49.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
80.230.230.12	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.199.10.52	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.138.69.157	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.116.97.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
141.255.42.69	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim	Block	1
5.29.193.198	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
87.70.55.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.179.170.73	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.255.145.131	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.235	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
41.187.92.101	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
2.53.156.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.98.245	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.98.245	Block	1
176.13.10.71	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
23.21.86.101	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/shared/usercontrols/headerupper/	Block	1
80.230.221.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.96.251	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.193.157	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
41.200.101.77	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

08-22-2016-21:04:02 to 08-22-2016-22:04:02