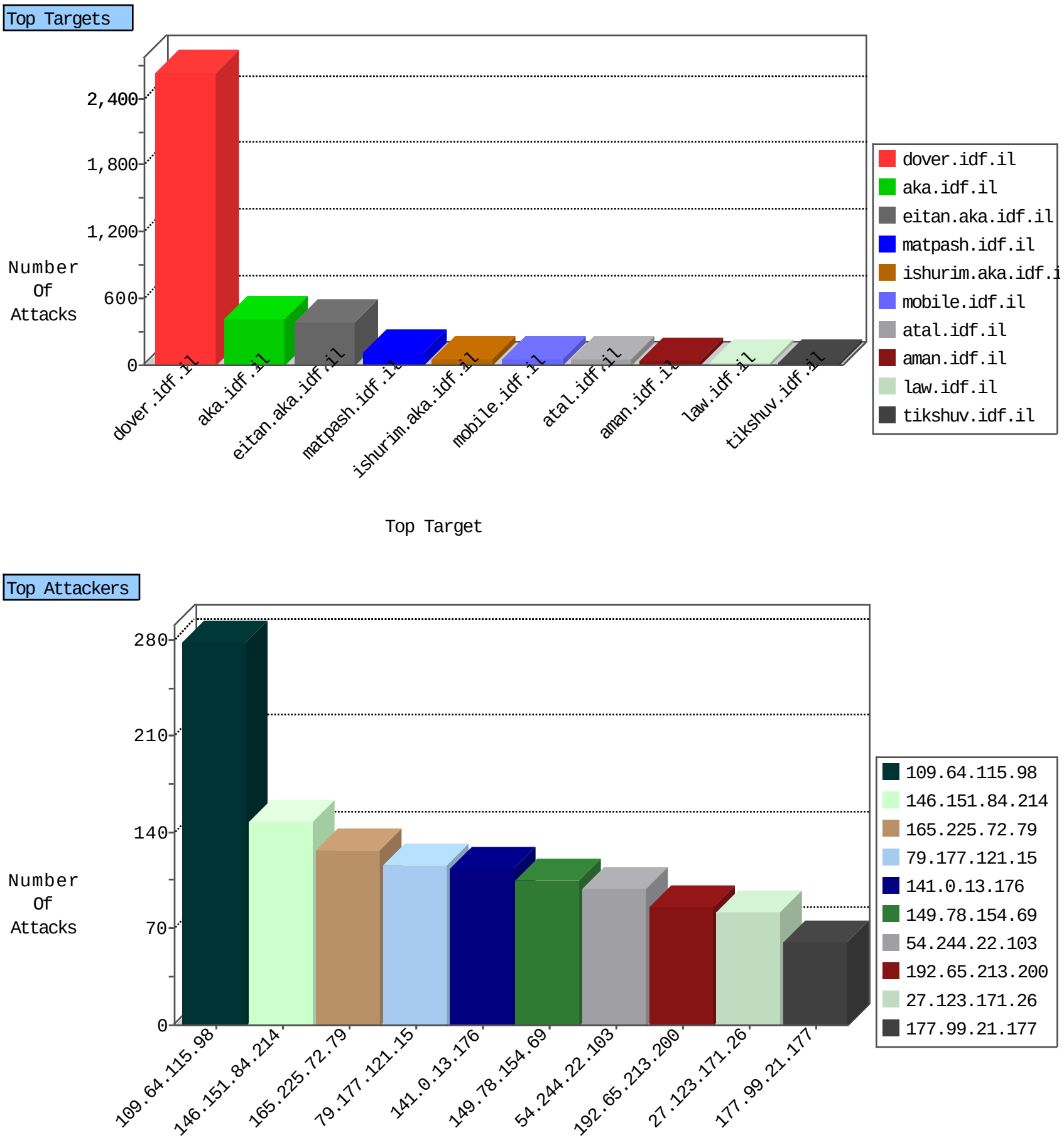
10-19-2015-00:04:07 to 10-19-2015-01:04:07

IDF Under Attack
Daily Report



10-19-2015-00:04:07 to 10-19-2015-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.116.64	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	111
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	59
84.109.154.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
176.12.141.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
27.123.171.26	Fiji	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
165.225.72.79	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
104.162.163.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
46.19.86.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.166.22.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.72.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.66.98.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.37.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
146.151.84.214	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
69.123.217.42	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.111.138.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
27.123.171.26	Fiji	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
84.228.87.3	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.114.226.46	Egypt	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.173.128.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
172.56.17.76	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.12.147.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
99.43.20.9	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.121.83.88	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.17.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.141.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.155.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.177.34.168	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
180.65.4.78	Korea, Republic of	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

10-19-2015-00:04:07 to 10-19-2015-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-00:04:07 to 10-19-2015-01:04:07

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	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
61.182.170.38	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	1
103.232.35.93	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -sS window 3072	1
178.37.243.103	147.237.76.148	Poland	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.232.35.93	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -f -sS	1
121.50.181.139	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
79.176.27.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	1
61.182.170.38	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	SERVER-IIS cmd.exe access	1
61.182.170.38	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
46.19.86.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	1
103.232.35.93	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN NMAP -sS window 2048	1
176.12.142.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.60.170.64	147.237.0.35	Portugal	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	1
61.182.170.38	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	1
61.182.170.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
105.108.180.184	147.237.77.216	Algeria	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1

10-19-2015-00:04:07 to 10-19-2015-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.115.98	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	279
146.151.84.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
165.225.72.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
141.0.13.176	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
192.65.213.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
27.123.171.26	Fiji	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
172.56.40.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
177.99.21.177	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.19.85.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
196.217.128.94	Morocco	147.237.77.216	dover.idf.il	drop		drop	54
46.19.86.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
71.29.11.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
5.22.130.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
2.54.164.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.173.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
93.65.155.197	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
142.255.113.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
213.57.129.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
5.29.84.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
73.3.64.220	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
70.192.193.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.177.121.15	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
5.102.250.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
69.123.217.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
24.114.71.176	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.182.117.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.166.22.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.12.146.60	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
176.12.141.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.76.127.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
1.129.97.115	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.121.15	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.121.15	Block	78
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	52
176.12.150.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
85.130.215.193	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	26
46.19.86.94	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
174.6.168.32	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
109.67.206.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
79.183.232.8	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	13
213.151.51.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/giyus/login.aspx	None	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	13
79.176.225.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
202.102.99.92	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	13
157.55.39.7	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	13
80.246.136.64	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	13
66.249.79.218	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	13
183.57.154.26	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/clientscripts/survey/survey.js?siteversion	Block	13
90.63.187.5	France	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	13
79.177.121.15	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 79.177.121.15	Block	13
213.57.185.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
62.24.181.134	United Kingdom	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	13
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sites/hoshen	Block	13
84.108.139.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
188.26.204.61	Romania	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
92.63.131.249	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/user	Block	13
213.57.185.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.185.185	Block	13
62.24.181.134	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	13
85.65.99.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17315.jpg	Block	13
109.67.175.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
79.179.15.112	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	13
213.57.211.70	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	13
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
176.12.146.60	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 102 cookies	Block	13
85.130.180.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	13
201.132.157.230	Mexico	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13