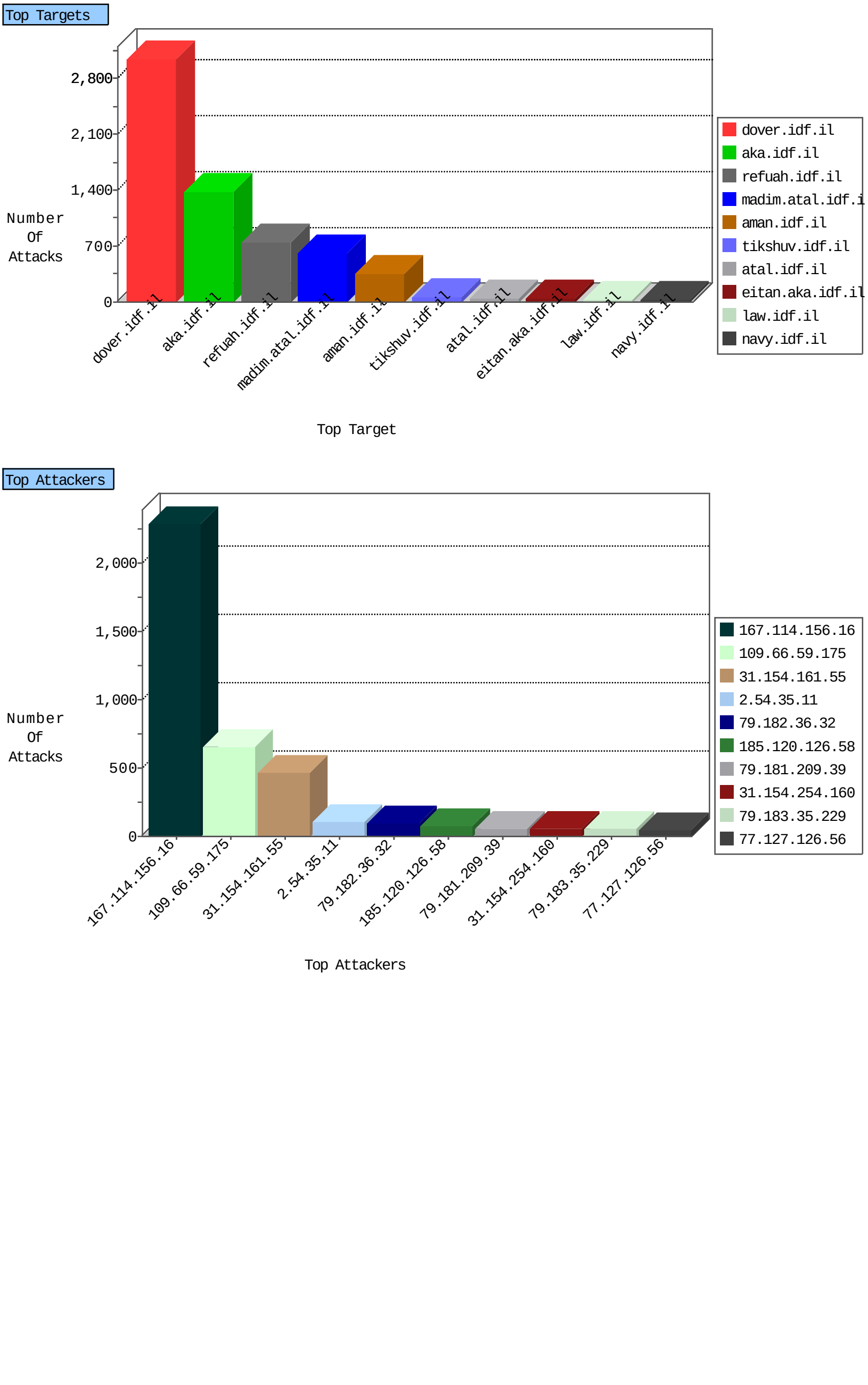
12-16-2015-21:04:05 to 12-16-2015-22:04:05

IDF Under Attack Daily Report



12-16-2015-21:04:05 to 12-16-2015-22:04:05

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	3311
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
172.58.169.154	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
123.194.2.31	Taiwan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
31.223.182.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
123.194.2.31	Taiwan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
70.199.116.226	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
72.38.11.210	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-16-2015-21:04:05 to 12-16-2015-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.19.46.6	United States	147.237.76.42	refuah.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
151.80.31.137	Italy	147.237.0.34	tikshuv.idf.i	C228: HTTP: AhrefBot crawler	Block	1

12-16-2015-21:04:05 to 12-16-2015-22:04:05

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
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.39	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
213.244.119.251	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.196	Sweden	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.17.14.46	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1

12-16-2015-21:04:05 to 12-16-2015-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.59.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	653
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
89.139.187.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
80.178.157.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
31.168.155.160	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.182.36.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	30
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
79.182.36.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
79.182.36.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
84.110.35.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
85.250.25.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
85.250.123.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	18
84.110.35.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
109.160.208.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
79.178.36.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
79.177.108.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
95.86.110.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.182.36.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.109.31.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
176.12.148.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
109.65.163.58	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
31.168.220.131	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	15
79.183.35.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	15
95.86.110.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	14
109.186.172.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.12.43.87	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.250.123.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
77.127.126.56	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.181.209.39	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
109.186.172.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
185.3.146.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.12.43.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
89.138.125.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.65.187.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.181.209.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
109.64.25.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.127.89.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.117.63.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.127.126.56	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.65.160.242	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.116.134.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.196.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.109.31.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.177.202.109	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.67.4.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

12-16-2015-21:04:05 to 12-16-2015-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.161.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	267
31.154.161.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
2.54.35.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
2.54.35.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
31.154.161.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	27
213.8.204.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
94.159.141.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.64.25.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
37.142.239.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.12.160.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
85.144.155.243	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
85.144.155.243	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
157.55.39.194	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
185.32.179.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.19	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
85.130.183.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
17.138.57.96	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list5.htm	Block	1
79.179.146.223	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20140-he/idfgdover.aspx	Block	1
89.139.187.214	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.11.221	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.142.217.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.78.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	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
54.153.33.233	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
41.141.92.129	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=wy0nxmurzzkjhefmituofznbqea-	Block	1
79.179.146.223	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
176.13.0.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
93.172.167.204	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
46.19.86.96	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
83.130.113.213	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
157.55.39.33	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
79.176.180.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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
46.19.85.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding Ibjg9UI(IeM.Ktr*CLf2MdpUf)1nJWfcx& in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
79.179.230.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
176.13.13.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
66.249.66.132	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.160.208.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.167.204	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
46.117.237.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
37.212.245.110	Belarus	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
212.179.163.75	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1

12-16-2015-21:04:05 to 12-16-2015-22:04:05