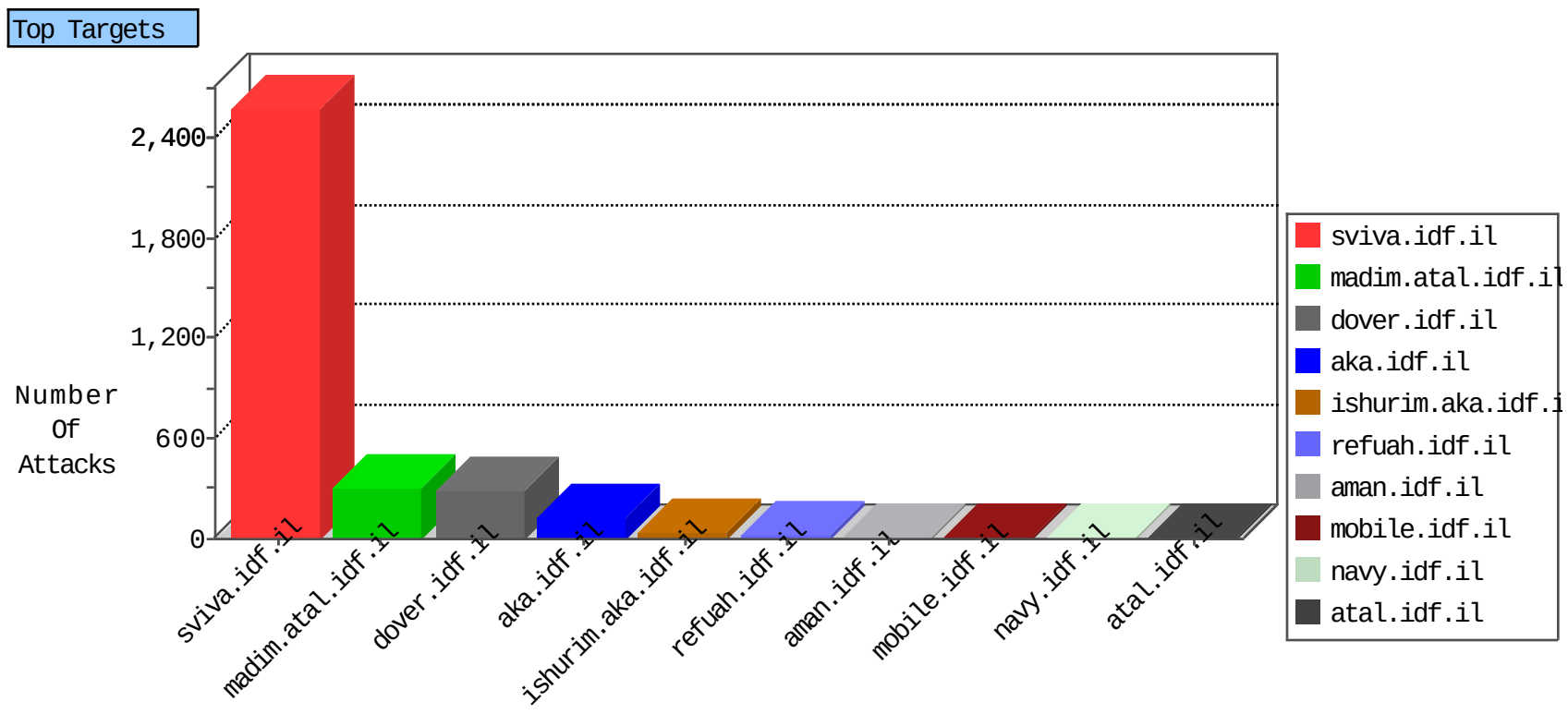
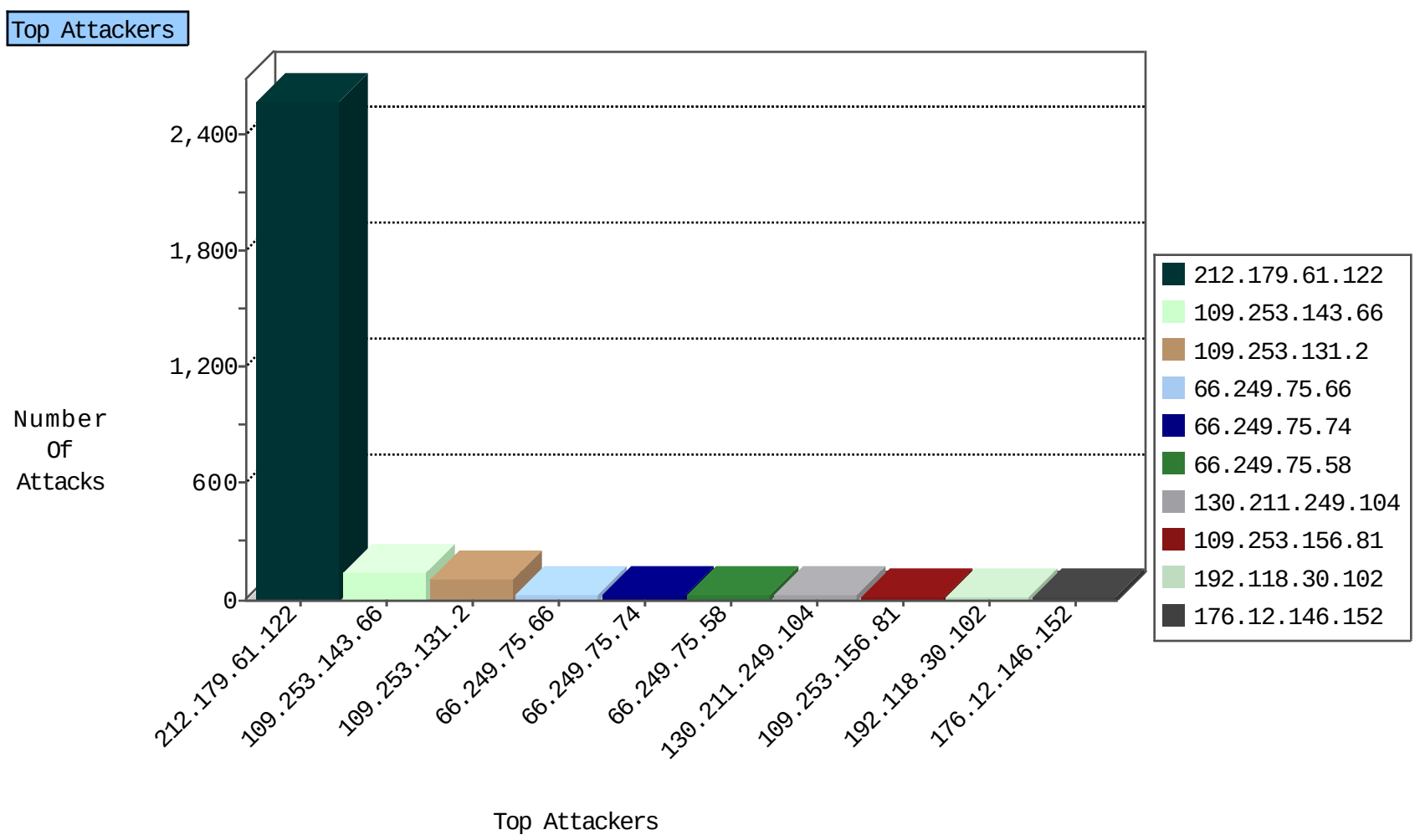
04-02-2015-10:03:04 to 04-02-2015-11:03:04

IDF Under Attack
04-02-2015-10:03:04

Top Targets



Top Attackers



04-02-2015-10:03:04 to 04-02-2015-11:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
87.69.162.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
149.78.202.243	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
107.154.64.10	United States	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	1
124.232.142.220	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-02-2015-10:03:04 to 04-02-2015-11:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
130.211.249.104		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
130.211.249.104		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	10
218.6.132.45	China	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.245	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
218.6.132.45	China	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.222	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-02-2015-10:03:04 to 04-02-2015-11:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
130.211.249.104		147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
186.67.150.139	Chile	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.210	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
185.32.177.218	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
109.67.186.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
94.188.255.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -f -sS	1
84.94.89.226	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.31.253	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.30	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.91.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
187.217.112.50	Mexico	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.38.33	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
185.32.178.71	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
149.88.136.140	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
109.66.20.216	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 2048	1
87.236.215.124	United Kingdom	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
217.66.232.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.27	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	Germany	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
2.54.187.11	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-02-2015-10:03:04 to 04-02-2015-11:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.122	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	2572
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.146.152	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
212.117.136.7	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.137.252	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.138.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.138.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
84.95.49.252	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	9
176.12.146.203	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
2.54.169.126	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
46.19.86.135	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.149.209	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
65.55.210.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
87.69.7.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.145.221	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.54.169.126	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
193.43.245.250	Israel	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	5
2.54.169.126	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.162.93.51	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
193.43.246.250	Israel	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
212.199.251.227	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
85.64.227.228	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
193.43.244.102	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	3
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
155.94.254.133		147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.253.132.106	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	2
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
209.88.198.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.189	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
212.179.195.66	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
85.64.227.228	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.78	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
193.43.246.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
89.248.172.57	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
199.203.93.50	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.65.23.67	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.218.206.115	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.143.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
109.253.131.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
109.253.156.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
109.253.144.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
109.253.130.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
109.253.156.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
109.253.133.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
62.219.137.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	5
85.250.44.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
88.198.48.46	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	2
80.246.133.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
130.211.249.104		147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.116.184.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
84.108.77.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.50.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
178.208.197.154	Gibraltar	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
62.219.229.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.146.229.158	Russian Federation	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
2.54.57.217	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
185.32.179.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	1
54.221.199.147	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
95.175.35.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper	Block	1
199.203.93.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$ctl00$cphMain$contentMainArea$btnPrevPhase in www.aka.idf.il/homas/site/homasformphase2.aspx	None	1
164.138.119.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
54.197.15.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/september/12.stm	Block	1
89.101.218.194	Ireland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
2.54.164.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
81.218.118.124	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.75.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1218-3.stm	Block	1
134.191.232.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
109.65.167.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$txtSearch in www.aka.idf.il/main/sachar/	None	1
54.225.104.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	1
87.68.72.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
46.120.136.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
207.241.229.214	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.204.20.249	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
89.101.218.194	Ireland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
5.29.55.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0227-2.stm	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kenesatuda	Block	1
134.191.232.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/webresource.axd	None	1
87.69.12.236	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1