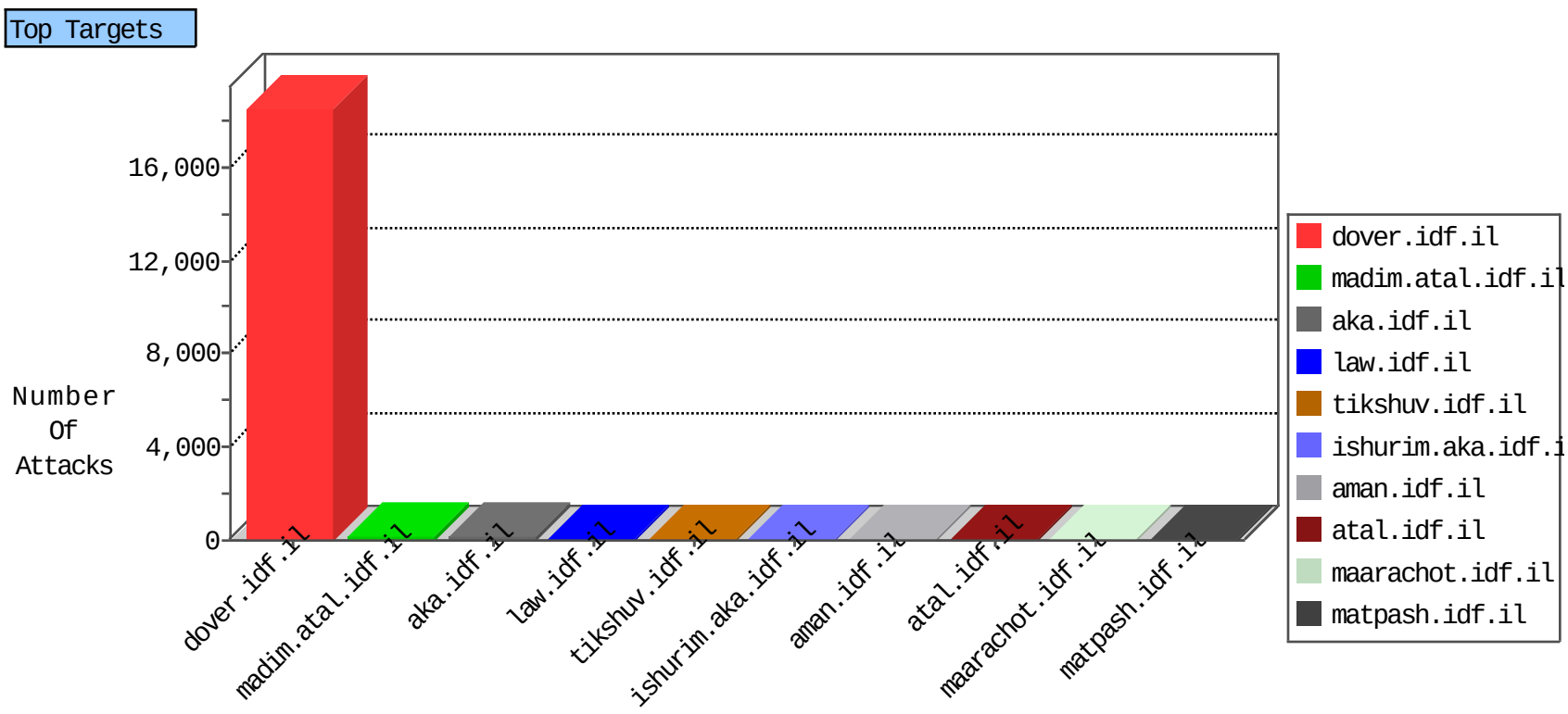
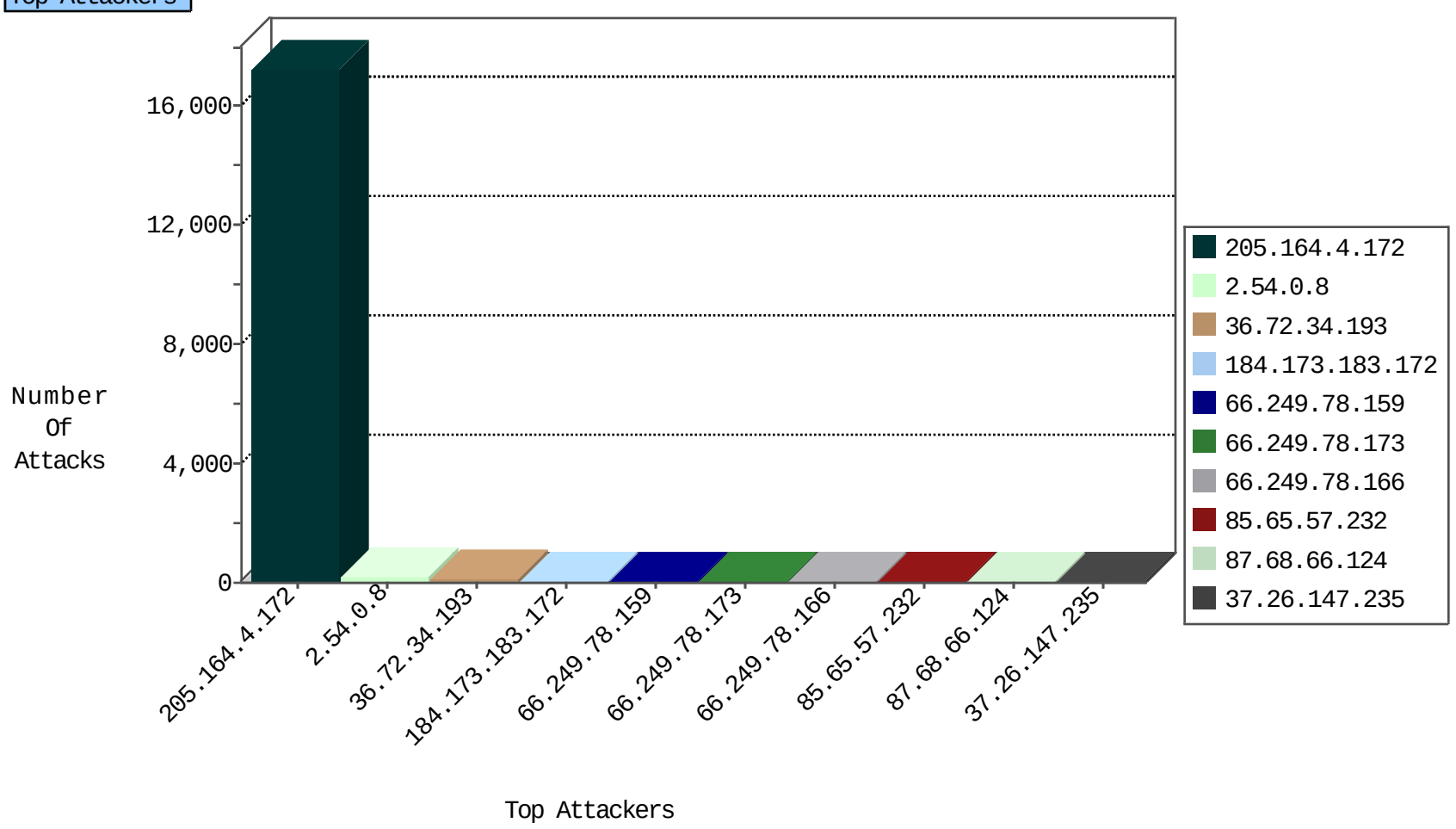
05-02-2015-18:03:02 to 05-02-2015-19:03:02

IDF Under Attack
05-02-2015-18:03:02

Top Targets



Top Attackers



05-02-2015-18:03:02 to 05-02-2015-19:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	523
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	324
77.125.135.21	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	226
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	145
205.164.4.172	United States	147.237.77.216	dover.idf.il	DOS-HOIC-TCP-80-gbo	forward	113
149.88.83.251	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
205.164.4.172	United States	147.237.77.216	dover.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	21
93.172.187.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
93.172.187.169	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
98.244.35.162	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
36.72.34.193	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.14.228.158	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.147.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
98.203.152.13	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.22.129.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-02-2015-18:03:02 to 05-02-2015-19:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	77
193.37.128.117	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
5.102.203.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.165.220.229	Germany	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.165.200	United States	147.237.77.121	e.navy.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
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.64.176.215	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-18:03:02 to 05-02-2015-19:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
205.164.4.172	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	37
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.22.130.248	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.183	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
5.22.129.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
119.92.202.251	Philippines	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.68	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.68	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.205.123	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
189.203.215.145	Mexico	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
182.72.109.162	India	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
119.92.202.251	Philippines	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.21.68	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.205.123	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.205.123	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
205.164.4.172	United States	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	1
5.135.199.12	France	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
189.203.215.145	Mexico	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
189.203.215.145	Mexico	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
178.32.251.100	France	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

05-02-2015-18:03:02 to 05-02-2015-19:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
205.164.4.172	United States	147.237.77.216	dover.idf.i	SAM rule	drop	drop	17029
205.164.4.172	United States	147.237.77.216	dover.idf.i		drop	drop	100
36.72.34.193	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	90
85.65.57.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
87.68.66.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
205.164.4.172	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.85.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
94.216.142.184	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
93.173.11.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
37.26.147.235	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
63.78.207.135	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
217.103.124.188	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
62.128.48.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
79.179.141.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
46.120.77.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.86.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
84.228.152.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
79.183.176.206	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
84.109.12.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
79.182.50.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
36.72.34.193	Indonesia	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	9
109.186.166.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
87.69.19.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
84.228.201.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.85.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
188.120.148.242	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
36.72.34.193	Indonesia	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
109.65.154.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
36.72.34.193	Indonesia	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	7
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
88.182.94.184	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
37.8.46.107	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.85.97	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.0.8	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.0.8	Block	192
5.22.130.174	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	4
77.125.135.21	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.120.206.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.206.73	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	2
149.88.58.156	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
37.26.147.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.153.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/qanda	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/590-he/patzar.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
87.69.19.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
5.22.130.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.67.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
37.187.56.81	France	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
149.78.108.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.130.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.29.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unknown Parameter 98160f90 in aka.idf.il/giyus/	None	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-4691-he/patzar.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13091-en/dover.aspx forcerecrawl: 0	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	1
89.139.29.118	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
5.29.94.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus.	Block	1
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/news.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/12.stm	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
37.187.56.81	France	147.237.72.156	aman.idf.il	Illegal HTTP Version + url + ' HTTP/1.1	Block	1
149.78.216.85	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.110.8.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.54.133.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
207.46.13.109	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
180.76.4.36	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/doctor	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
36.72.34.193	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
95.87.72.86	Kyrgyzstan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	1
77.125.23.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0318-3.stm	Block	1
37.247.36.75	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
87.68.38.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1

05-02-2015-18:03:02 to 05-02-2015-19:03:02