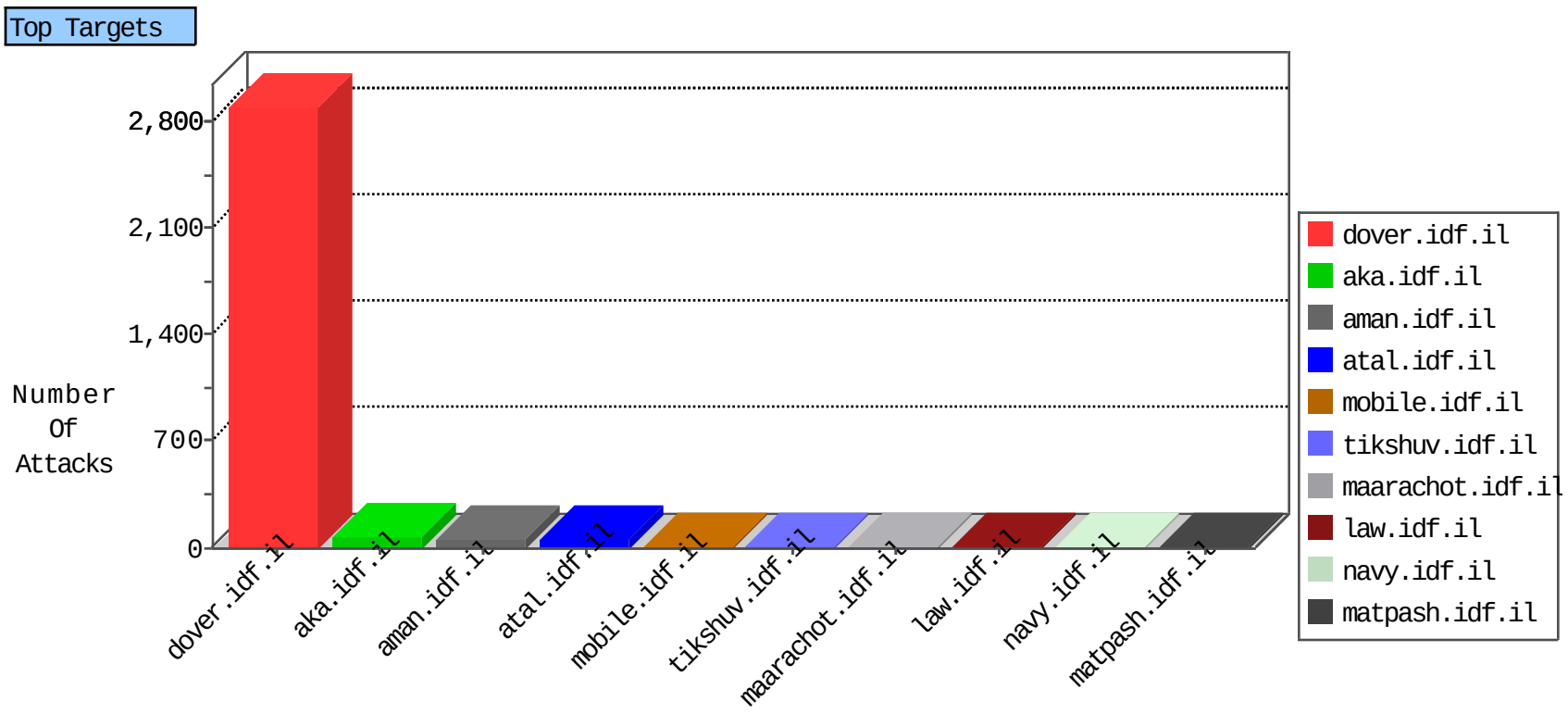
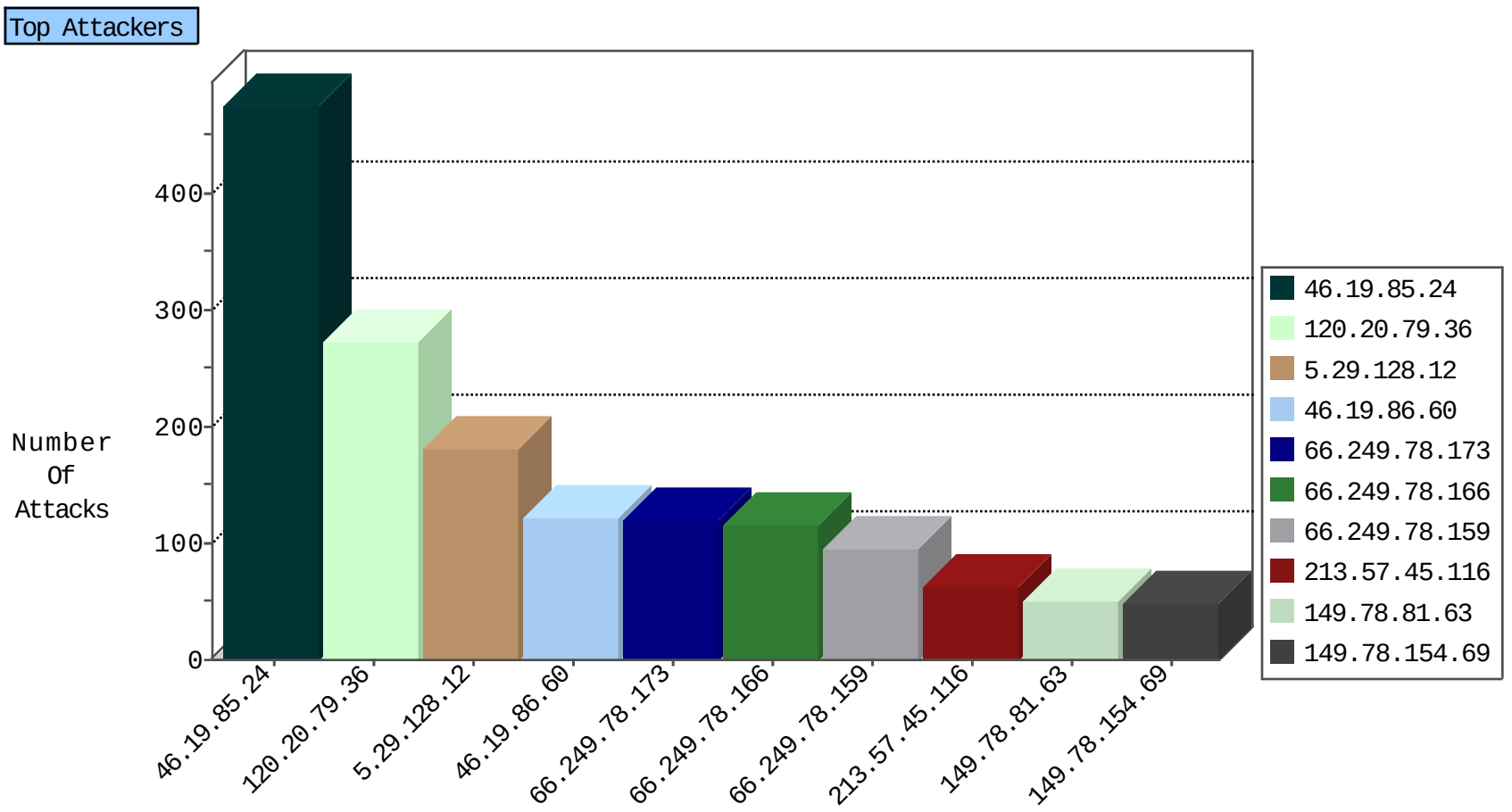
05-02-2015-11:03:09 to 05-02-2015-12:03:09

IDF Under Attack
05-02-2015-11:03:09

Top Targets



Top Attackers



05-02-2015-11:03:09 to 05-02-2015-12:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3503
149.78.81.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	480
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	232
5.29.159.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.3.206.130	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
192.3.206.130	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

05-02-2015-11:03:09 to 05-02-2015-12:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.218.77.147	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.110.77.39	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
109.67.185.239	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
174.3.61.95	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.60	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
185.32.179.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.28	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-11:03:09 to 05-02-2015-12:03:09

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	6
37.142.141.107	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.121.116.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.135.199.12	France	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
76.76.106.42	Canada	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.42	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.141.165.41	Germany	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
178.32.251.100	France	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

05-02-2015-11:03:09 to 05-02-2015-12:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	475
120.20.79.36	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	273
5.29.128.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	181
46.19.86.60	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	90
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
213.57.45.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
72.204.162.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
176.12.148.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
80.246.133.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.148.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
84.111.138.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
46.121.205.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
77.125.145.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.116.211.28	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	26
213.57.139.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
15.203.169.107	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.86.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
210.89.41.213	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.67.167.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
109.67.185.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
94.159.152.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
79.177.57.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
84.108.86.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.19.86.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.178.139.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.160.190.162	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
213.57.150.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.116.98.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.182.52.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
194.90.167.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
174.129.18.134	United States	147.237.77.176	matpash.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.120.175.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
174.129.18.134	United States	147.237.77.176	matpash.idf.il	Post Request - Missing Content Type	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	2
149.78.130.5	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
85.64.247.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim	Block	1
109.67.185.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
79.178.149.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
157.55.39.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers/paratroopers.stm	Block	1
46.229.164.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/printpreview/default.asp	Block	1
5.28.151.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
213.57.45.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.65.157.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
176.12.142.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter 6683f660 in www.aka.idf.il/main/home/default.aspx	None	1
109.160.190.162	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
37.142.80.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
79.180.124.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.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
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-4236-he/patzar.aspx	Block	1
157.55.39.53	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
46.229.164.111	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper	Block	1
217.132.65.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
93.172.172.39	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
176.12.150.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/mobile/	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
109.253.146.85	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
46.116.211.28	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1
84.228.19.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.78	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	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
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/news	Block	1
37.16.72.139	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1