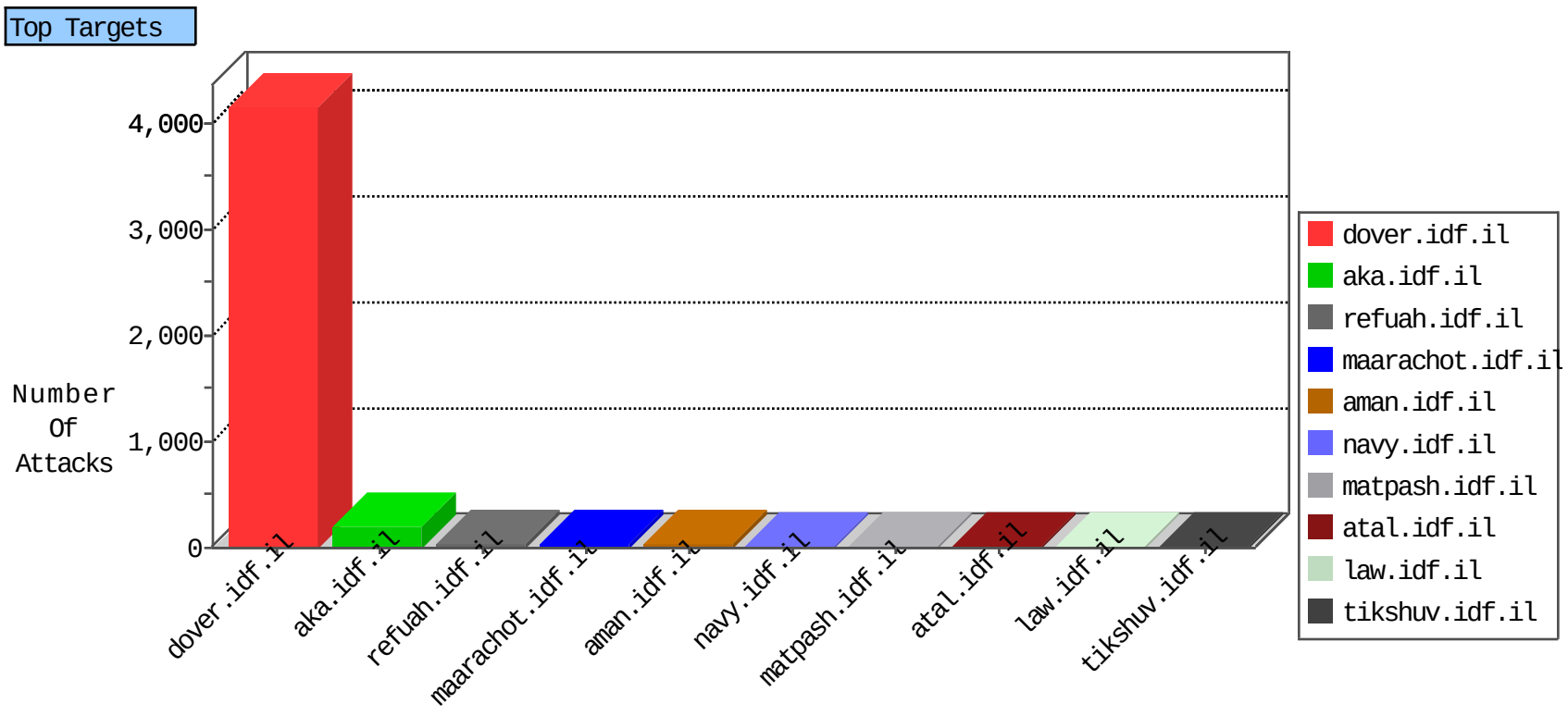
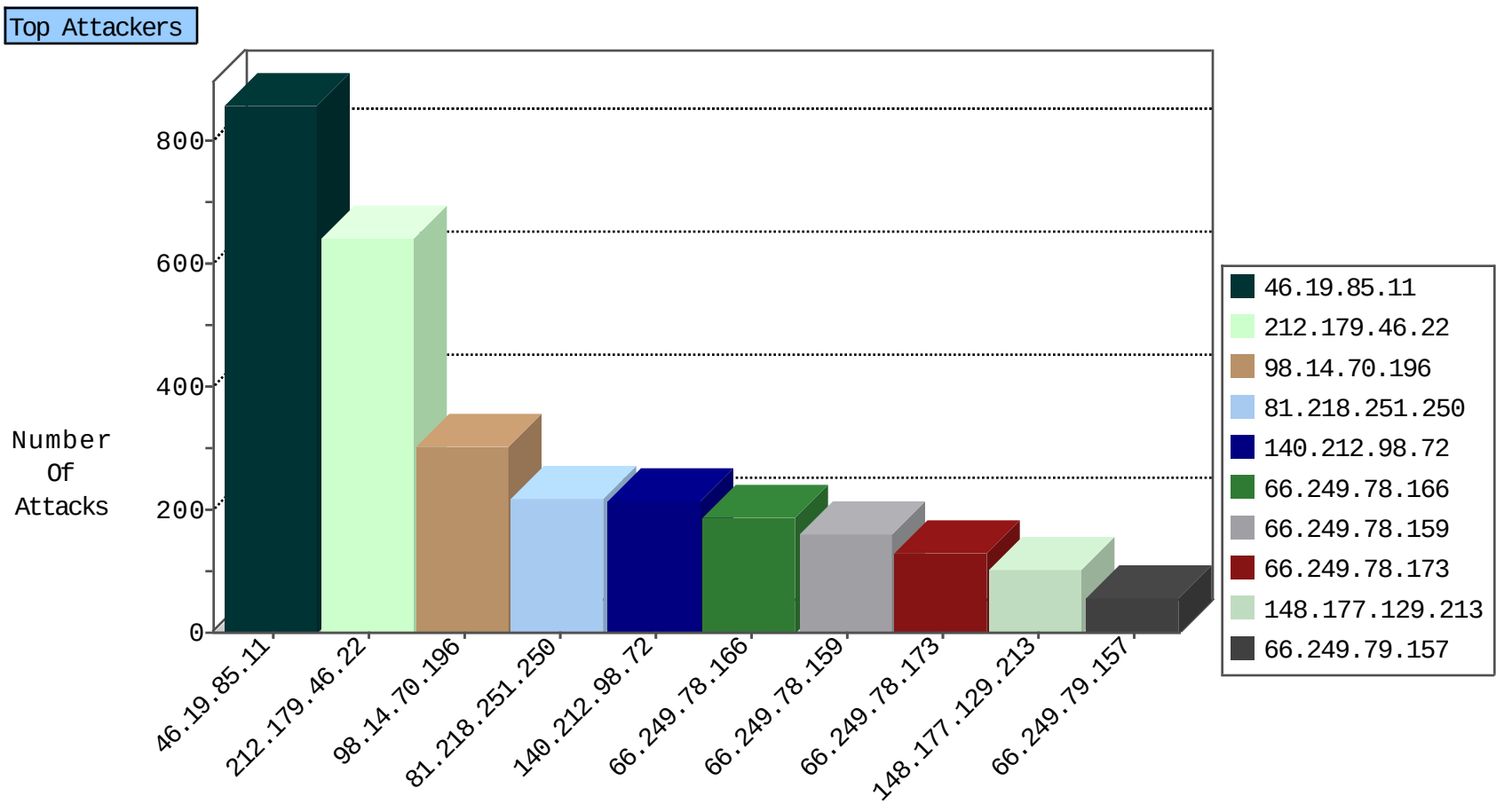
04-16-2015-07:03:08 to 04-16-2015-08:03:08

IDF Under Attack
04-16-2015-07:03:08

Top Targets



Top Attackers



04-16-2015-07:03:08 to 04-16-2015-08:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.39	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	729
84.228.48.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
85.250.211.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
89.138.51.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.102.141.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.102.141.251	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	1

04-16-2015-07:03:08 to 04-16-2015-08:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.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
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.182	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1

04-16-2015-07:03:08 to 04-16-2015-08:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.13	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
85.17.87.33	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.55.55.59	Poland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.30.41	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
8.29.144.205	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.30.41	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.210.3.64	Malaysia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
95.242.63.20	Italy	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
93.173.25.176	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
8.29.144.205	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.30.41	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
111.13.30.109	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
95.242.63.20	Italy	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-16-2015-07:03:08 to 04-16-2015-08:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	860
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	643
98.14.70.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	304
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220
140.212.98.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	130
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	118
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	100
66.249.79.157	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
109.253.137.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
93.173.25.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
77.125.223.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.253.129.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
24.148.95.83	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
109.190.127.39	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.85.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.253.131.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
79.180.134.2	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	18
135.0.63.132	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
108.27.115.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
120.17.57.237	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.253.147.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.179.46.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
2.54.5.125	Israel	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.158.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.140.226	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
95.86.111.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
132.71.84.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.109.46.25	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
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	12
79.180.134.2	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
109.253.149.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
77.127.223.205	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	5
82.166.125.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.166.125.198	Block	3
80.246.133.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
193.169.188.90	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	2
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
91.200.12.54	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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
207.46.13.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.5.204.20	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
81.218.200.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.79.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8452-he/navy.aspx	Block	1
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
180.76.5.58	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/896-he/cogat.aspx	Block	1
94.223.189.155	Germany	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
77.125.151.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.71	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/kamlar/	None	1
66.249.79.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8640-he/navy.aspx	Block	1
193.169.188.90	Ukraine	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
2.54.4.220	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1501-he/atal.aspx	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22721	Block	1
61.135.190.197	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
174.129.237.157	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.166.125.198	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
66.249.79.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8650-he/navy.aspx	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/clali.stm	Block	1
37.58.71.199	Netherlands	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.122.184	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.122.184	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
212.116.172.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	1
61.135.190.200	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
176.12.136.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.211.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
66.249.79.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
66.249.79.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
62.219.130.136	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
176.12.141.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1