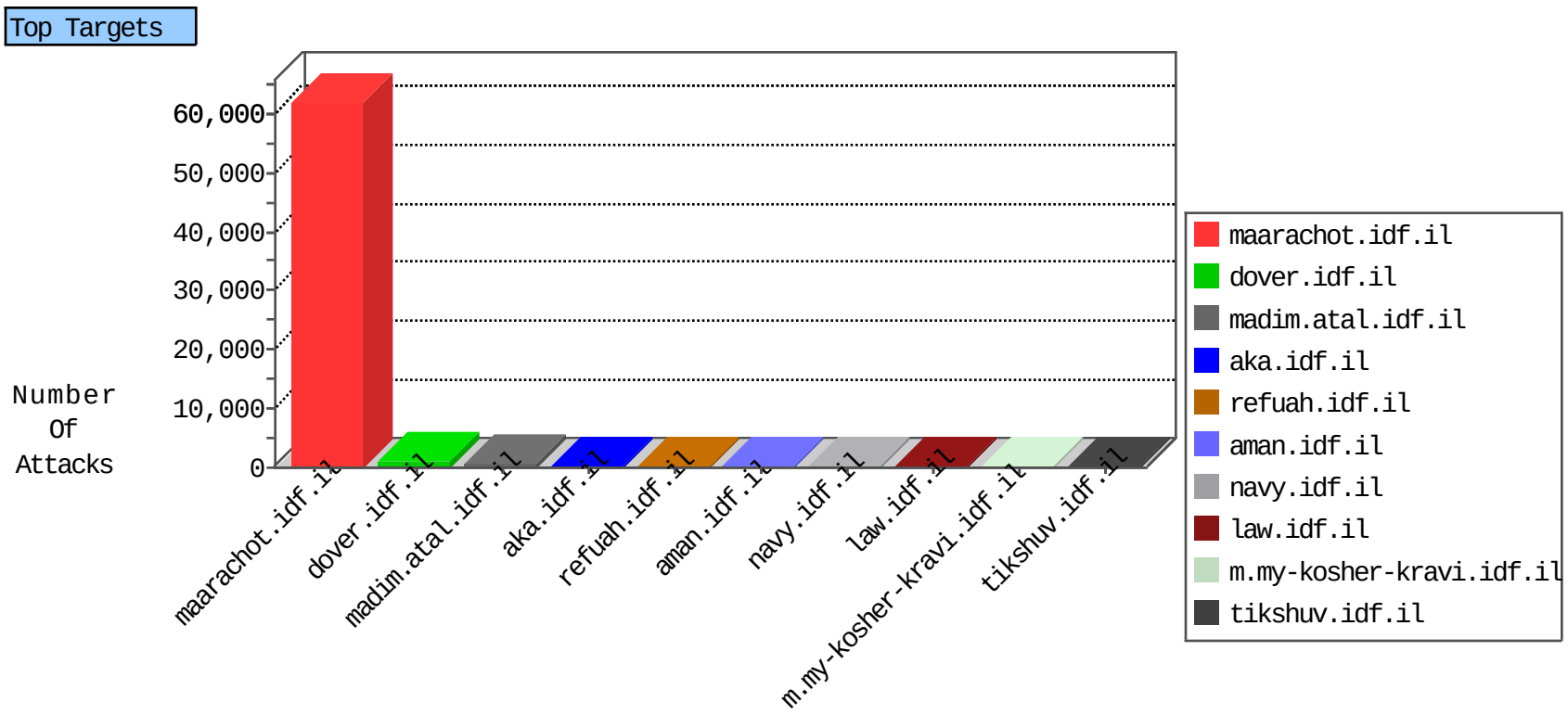
04-14-2015-21:03:01 to 04-14-2015-22:03:01

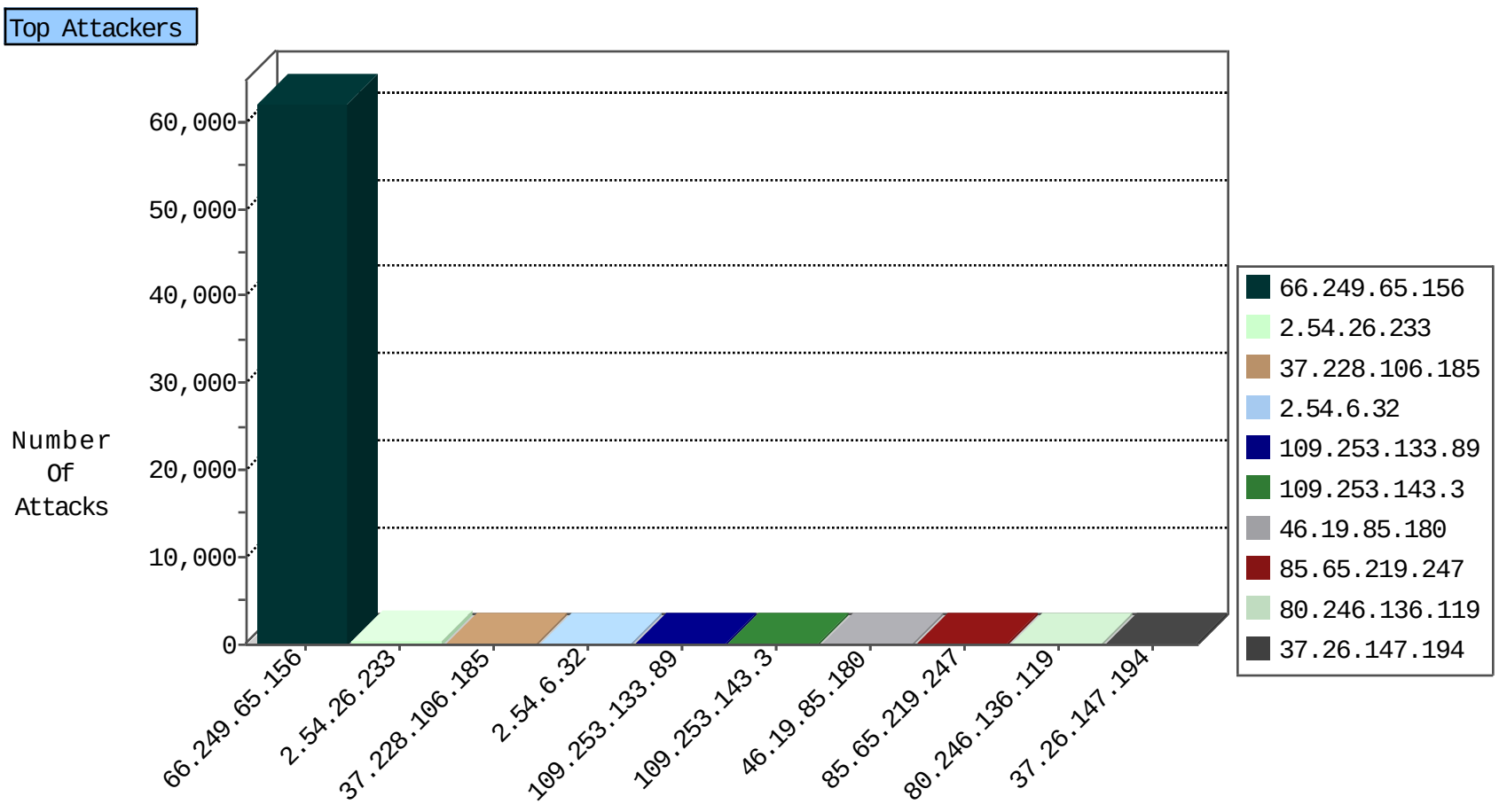
IDF Under Attack
04-14-2015-21:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

04-14-2015-21:03:01 to 04-14-2015-22:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.43	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1015
220.181.108.143	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	445
79.176.184.54	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
85.64.151.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
89.138.218.105	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2

04-14-2015-21:03:01 to 04-14-2015-22:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.219.247	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.64.151.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
149.78.114.241	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.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
85.25.43.94	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
170.140.105.65	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
87.69.242.228	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.187	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
178.241.82.191	Turkey	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
104.200.78.140		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
109.67.63.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
77.126.73.194	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-14-2015-21:03:01 to 04-14-2015-22:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	62200
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
194.90.216.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.141.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
104.171.114.254		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
50.97.52.130	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.241.153.80	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.241.153.80	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
168.235.154.235		147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
113.57.151.37	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
113.57.151.37	China	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
104.171.114.254		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.77	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.121.246.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.241.153.80	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
168.235.154.235		147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
122.228.207.77	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
113.57.151.37	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
109.253.147.10	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.77	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1

04-14-2015-21:03:01 to 04-14-2015-22:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.228.106.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
2.54.6.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
46.19.85.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.26.147.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
80.246.136.119	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
85.65.219.247	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.19.85.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
213.57.233.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.85.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.136.2	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
149.88.93.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
93.173.253.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
79.176.100.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
95.35.4.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
166.137.126.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
91.1.218.216	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
85.64.47.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
38.104.200.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.188.142.55	Croatia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.181.54.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
80.246.130.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.51.100.143	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.94.197.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
12.10.219.225	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.86.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.54.8.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
185.4.255.51	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.151.48.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
37.26.148.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
130.64.35.143	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
94.159.141.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.102.254.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
80.246.130.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.39.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
213.57.63.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
80.230.126.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.26.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	359
109.253.133.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
109.253.143.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
109.64.144.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.144.117	Block	16
95.149.0.2	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
37.26.147.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
109.160.180.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
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	4
80.246.130.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
109.160.200.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.4.255.51	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	2
149.88.13.182	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.29.150.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.196.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.48.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.179.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
182.118.54.14	China	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.65.56	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/925-he/navy.aspx	Block	1
109.64.144.117	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
46.120.56.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.94.204.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/gaash/pics.stm	Block	1
66.249.65.72	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
64.41.200.104	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
109.67.63.126	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.63.126	Block	1
37.26.146.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.242.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.65.58	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/927-he/navy.aspx	Block	1
109.64.144.117	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/function () { var c = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } els { var a = this[0] r 360; var e = a e 60; var g = math.round((this[2] * (100 - this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return [c, b, g];	Block	1
46.120.118.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
84.108.105.213	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.209	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.20	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
109.67.63.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
91.217.90.49	Ukraine	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/rom-0	Block	1
80.246.136.119	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
109.253.144.108	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.65.60	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1161-he/navy.aspx	Block	1
46.120.120.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.83.78.223	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0306-2.stm	Block	1
85.64.72.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
180.76.4.156	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.65.22	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
93.172.23.108	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
82.166.81.221	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
212.199.205.69	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1