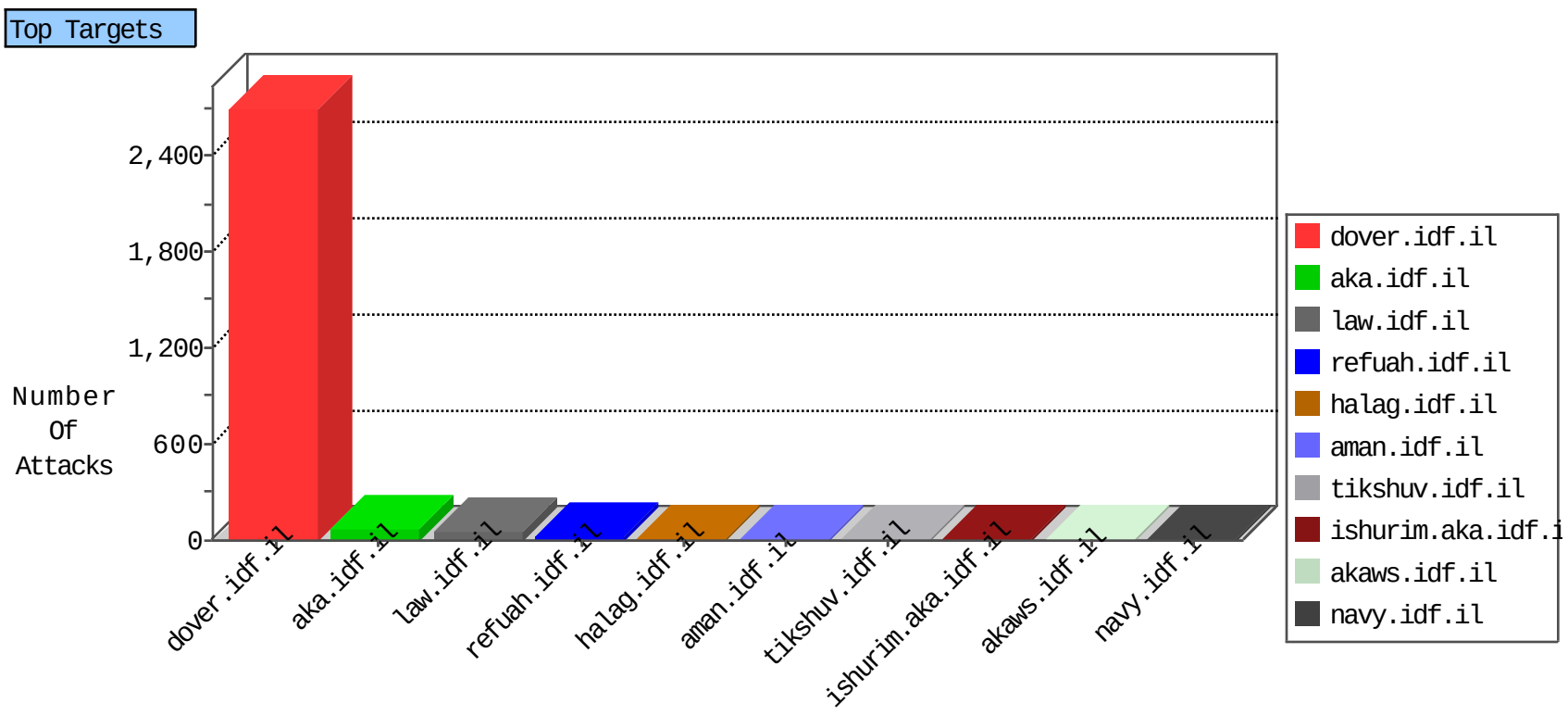
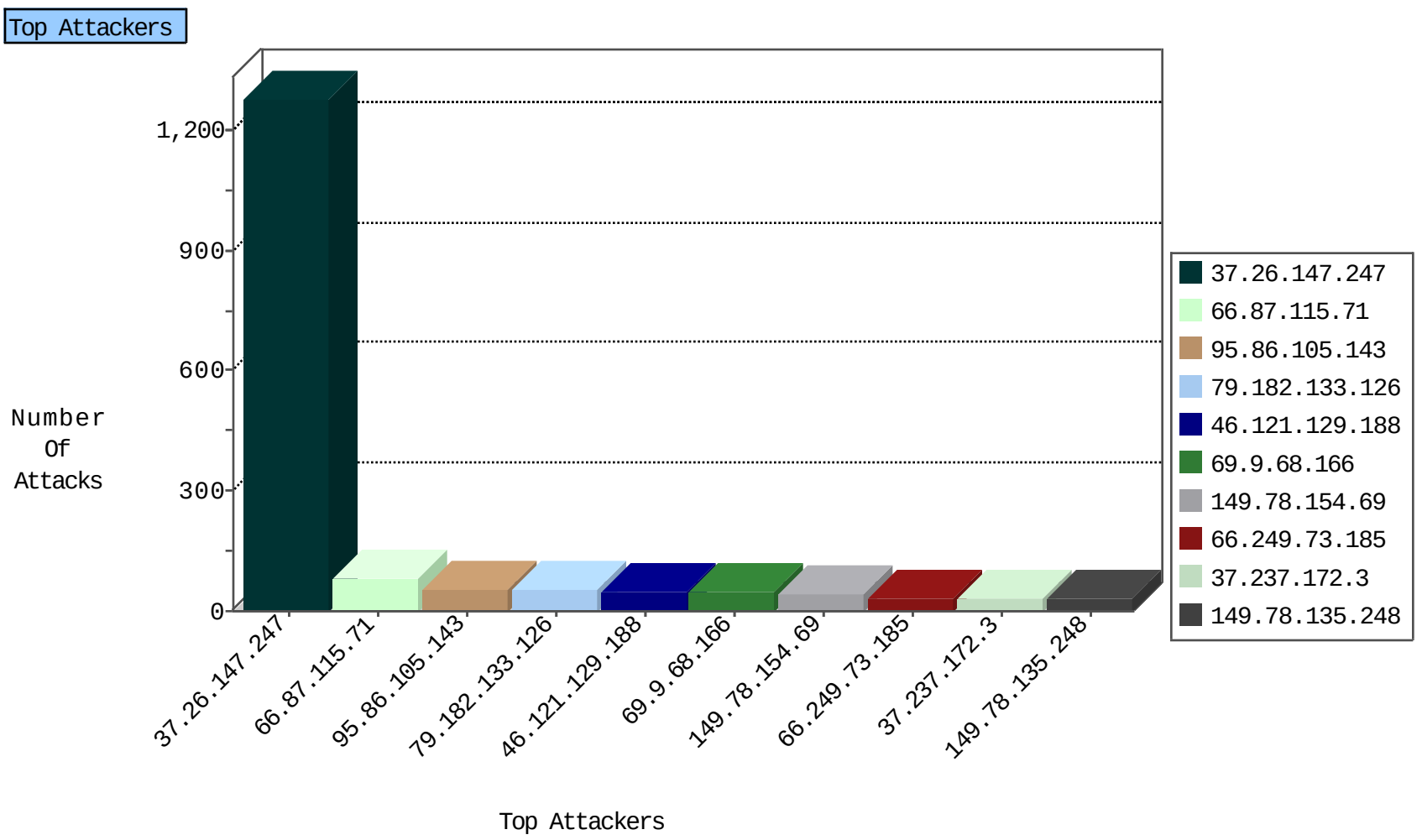
05-10-2015-00:03:07 to 05-10-2015-01:03:07

IDF Under Attack
05-10-2015-00:03:07

Top Targets



Top Attackers



05-10-2015-00:03:07 to 05-10-2015-01:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
185.32.178.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
109.253.141.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
220.181.108.91	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	63
89.138.74.135	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.86.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-10-2015-00:03:07 to 05-10-2015-01:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.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
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.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
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.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
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1

05-10-2015-00:03:07 to 05-10-2015-01:03:07

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
66.249.67.126	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
37.142.65.248	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.31.13	Israel	147.237.77.226	www.chamatz.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
61.160.215.26	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.215.26	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
58.137.55.5	Thailand	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
121.46.0.125	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
58.137.55.5	Thailand	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
121.46.0.125	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
203.170.75.2	Pakistan	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.215.26	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
61.160.215.26	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
58.137.55.5	Thailand	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
121.46.0.125	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
58.54.134.13	China	147.237.76.31	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.130		147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
203.170.75.2	Pakistan	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

05-10-2015-00:03:07 to 05-10-2015-01:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.26.147.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1282
66.87.115.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
95.86.105.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
79.182.133.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
46.121.129.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
69.9.68.166	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
37.237.172.3	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
109.253.134.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
149.78.135.248	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	29
212.45.46.32	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
212.179.213.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
79.176.144.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
37.237.172.88	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
37.237.172.196	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.86.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
188.161.179.17	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
84.109.3.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
185.26.182.28	Europe	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	16
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
37.26.147.219	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
135.0.63.132	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
71.176.225.94	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
188.227.238.173	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.87.130.150	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
80.246.130.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
37.237.172.53	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
172.56.11.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
84.229.45.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.237.172.89	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
37.237.172.160	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
79.180.68.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.237.172.238	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.237.172.104	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.237.172.42	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
77.126.175.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.73.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
37.142.65.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
85.250.125.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.237.172.27	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
89.138.74.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
37.26.146.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
37.237.172.163	Iraq	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
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	15
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	14
85.65.161.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
85.65.161.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
79.182.193.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	3
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
109.253.134.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
5.28.145.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	2
77.127.184.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
210.195.195.121	Malaysia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
71.176.225.94	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ air force	Block	1
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
109.160.133.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
210.195.195.121	Malaysia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
178.62.202.236	Netherlands	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
83.130.118.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.76.97.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
66.249.78.247	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
180.76.4.211	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
87.68.50.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15858-he/dover.aspx×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³â,ª×³Â§×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½	Block	1
5.255.253.93	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
83.222.232.214	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /	Block	1
212.179.42.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.79.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1537-8798-he/atal.aspx	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
180.76.5.71	China	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
89.169.43.217	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1
79.176.101.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/kishur/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
31.13.112.123	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6	Block	1
85.64.202.3	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
213.57.231.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.138.17.205	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
95.86.99.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	1
79.178.149.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1