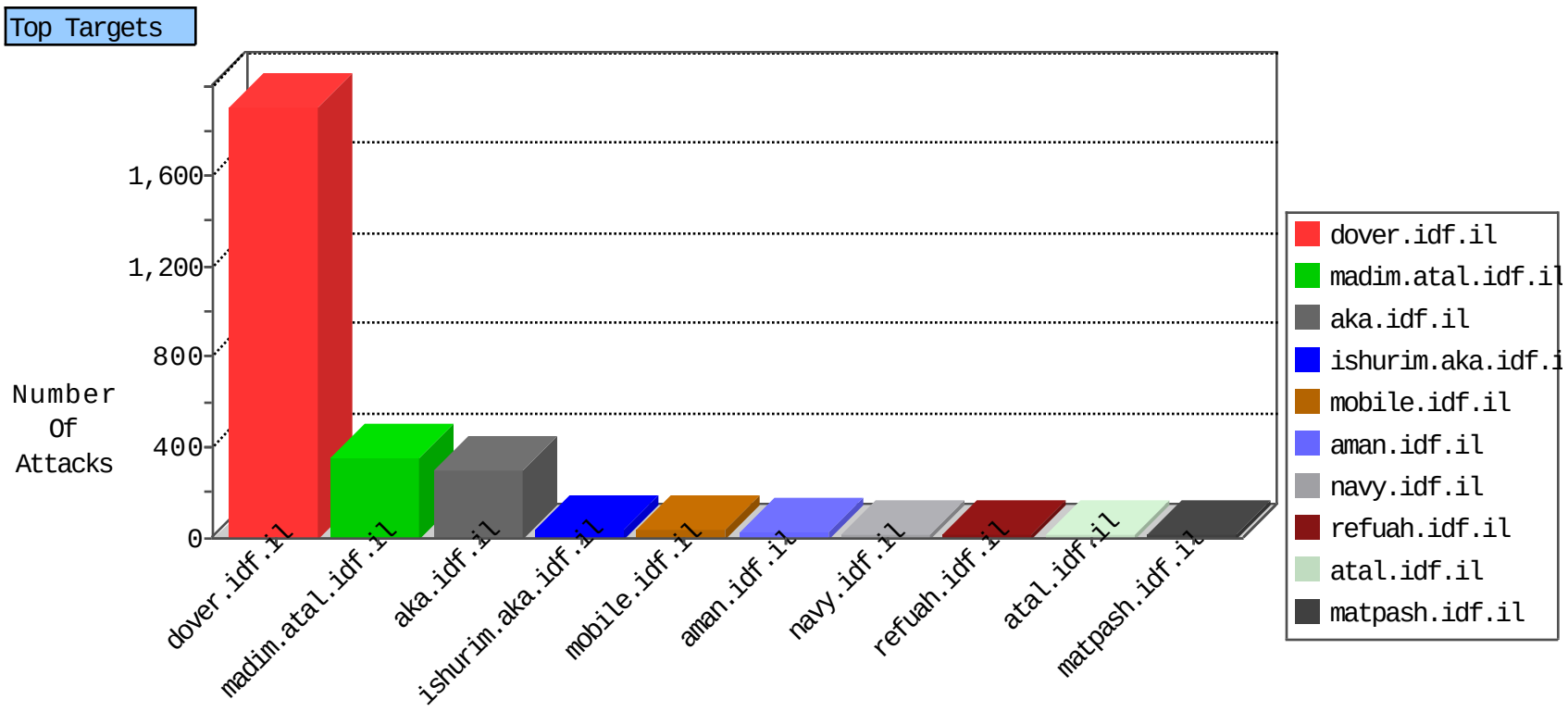
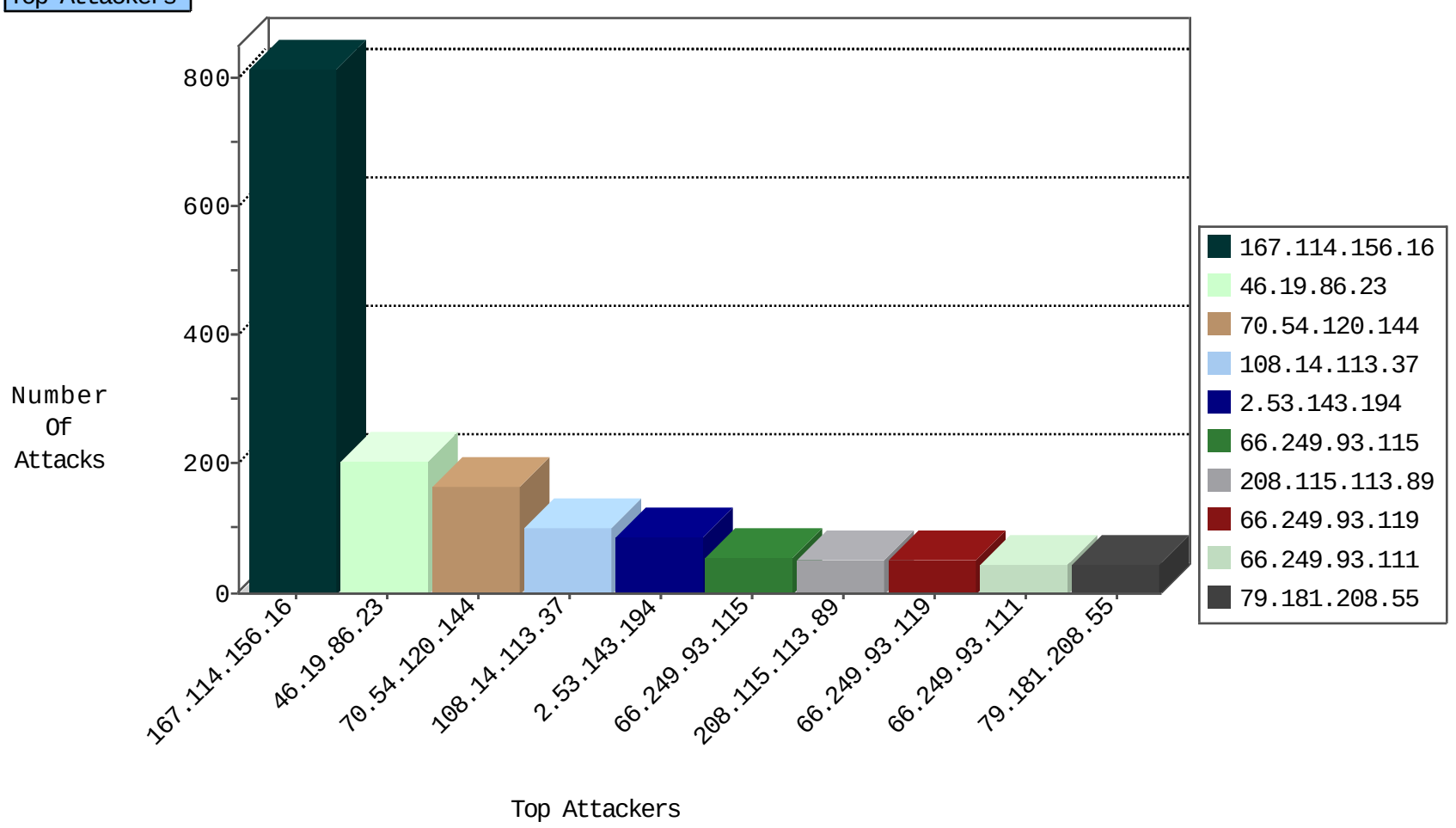
05-04-2016-15:04:04 to 05-04-2016-16:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-04-2016-15:04:04 to 05-04-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14991
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	796
154.103.210.153	Sudan	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	7
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.56	Lithuania	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
82.166.184.148	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.56	Lithuania	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.158.166	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.118.223.13	Lebanon	147.237.77.61	e.cogat.idf.il	L4 Source or Dest Port Zero	drop	1

05-04-2016-15:04:04 to 05-04-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

05-04-2016-15:04:04 to 05-04-2016-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.208.160.181	147.237.77.216	Romania	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.158	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
192.118.12.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
46.121.154.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
2.55.191.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
2.53.56.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
178.62.75.195	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
154.103.210.153	147.237.77.216	Sudan	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.242.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
84.228.19.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
79.183.191.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
5.102.254.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
2.53.148.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.46.25.59	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.46.25.59	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.157.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-04-2016-15:04:04 to 05-04-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	367
70.54.120.144	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	164
108.14.113.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
79.181.208.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
195.226.71.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
194.56.4.51	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.26.148.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
199.203.179.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
78.150.125.16	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
82.145.217.194	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
24.229.110.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.142.250.243	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.53.60.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.14.164.58	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.228.237.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
94.199.151.22	United Kingdom	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.1.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop		drop	10
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop		drop	10
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.180	Europe	147.237.72.166	aka.idf.il	drop		drop	8
66.249.93.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.128.242	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.93.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.181.208.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.35.194.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.136.237	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	204
2.53.143.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
46.19.85.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.207.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.151.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.211.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.119.115.27	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
46.119.115.27	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.119.115.27	Block	5
2.53.191.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.73.75.191	Georgia	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.55.213.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.24.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.207	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
42.96.177.34	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
82.81.63.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
176.13.22.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.73.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.186.182.80	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
213.8.42.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
82.205.11.221	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.153.78	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3350.jpg	Block	1
62.210.148.247	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/tikshuv/index.htm-אתר	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method zN*}…±Õ,œTúôyó'„`éD˜	Block	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
207.46.13.106	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/news/	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.73.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.119.115.27	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
42.96.177.34	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 42.96.177.34	Block	1
213.8.204.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
83.68.225.42	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman'a=0	Block	1
2.53.153.78	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.153.78	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
74.82.47.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL [[#22]]¸s-×…¡k`üחחŸ1:4±	Block	1
94.199.151.22	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
80.246.139.25	Israel	147.237.76.39	mobile.meitav.idf.il	Multiple Untraceable SSL Sessions from 80.246.139.25 (Open Mode)	None	1
31.154.4.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 31.154.4.18	Block	1
212.143.90.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.143.90.173	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1076-he/אגף הטכנו לוגיה והלוגיסטיקה.aspx	Block	1
46.121.192.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
220.255.148.146	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1