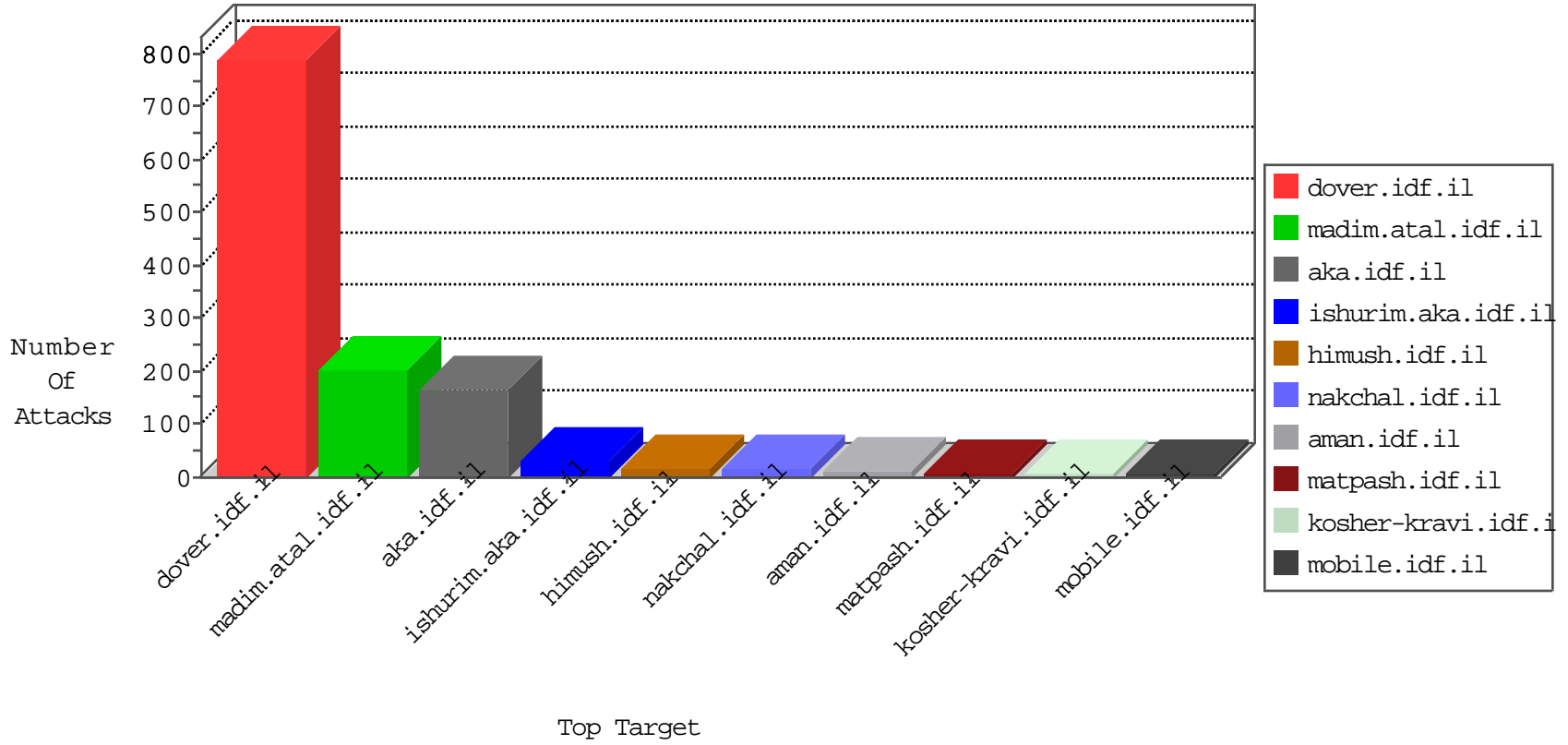


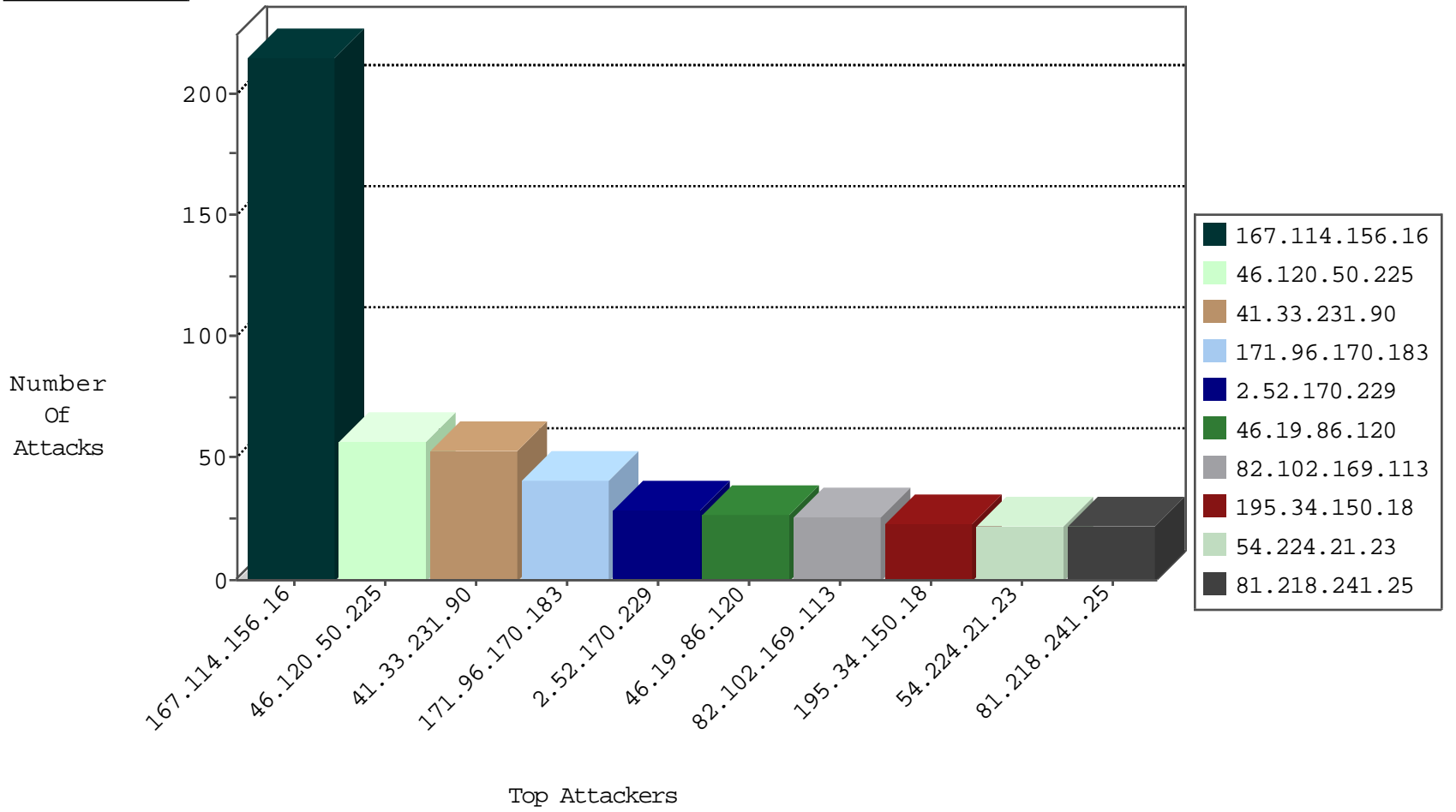
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	HTTP-POST-Segmented-DoS	dest-reset	8341
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	254
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	19
185.106.94.28		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.139	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.96	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
74.117.209.135	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
198.179.158.11	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.0.200	Cote D'Ivoire	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
42.118.49.51	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
183.230.52.199	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.6.71.154	147.237.76.201	Poland	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.36	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
176.13.21.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.2.140.139	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
90.2.140.139	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
220.149.30.163	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.84.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.101.186.178	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
74.117.209.135	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.0.200	Cote D'Ivoire	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
46.121.69.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
176.12.151.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.2.140.139	147.237.8.45	France	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
90.2.140.139	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
212.25.84.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
171.96.170.183	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.46.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
96.244.120.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.12.76	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.224	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	11
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.114.91.234	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.19.78.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
131.253.25.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
165.225.72.59	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.42.114	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
66.249.79.77	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.37.109	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
178.12.227.251	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.246.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.22.111.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	6
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
117.218.74.200	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.14.146.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.186.63.77	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.236.82.50	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
96.244.120.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.50.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.52.170.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.12.138.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.179.38.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.137.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.146.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.26.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
198.1.101.123	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.139.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
31.44.135.222	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 31.44.135.222	Block	2
2.54.39.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.26.27.42	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.26.27.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.149.148	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation returnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
211.123.214.30	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
5.15.193.149	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.112	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/kapatz/ã-âe"ã-âe?	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
89.139.174.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
207.46.13.172	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/894-en	Block	1
2.54.179.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct167 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.2	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
212.29.223.233	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
5.28.156.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.119	Block	1
95.57.87.143	Kazakstan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/1035-en/idfg.aspx	Block	1
46.117.18.38	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18863-en/dover.aspx.	Block	1
2.54.180.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.95.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3097.pdfã¼	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.246.140.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1