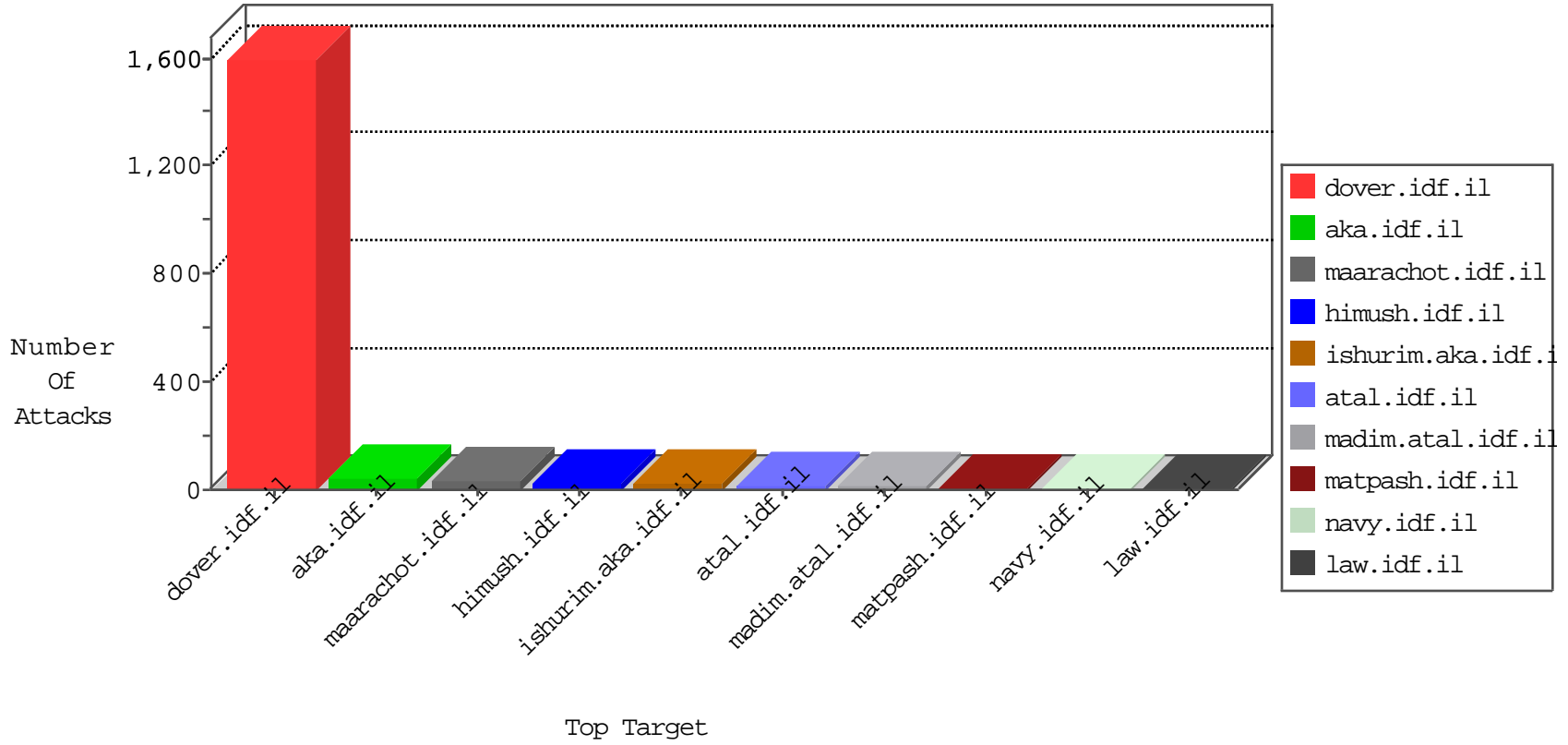


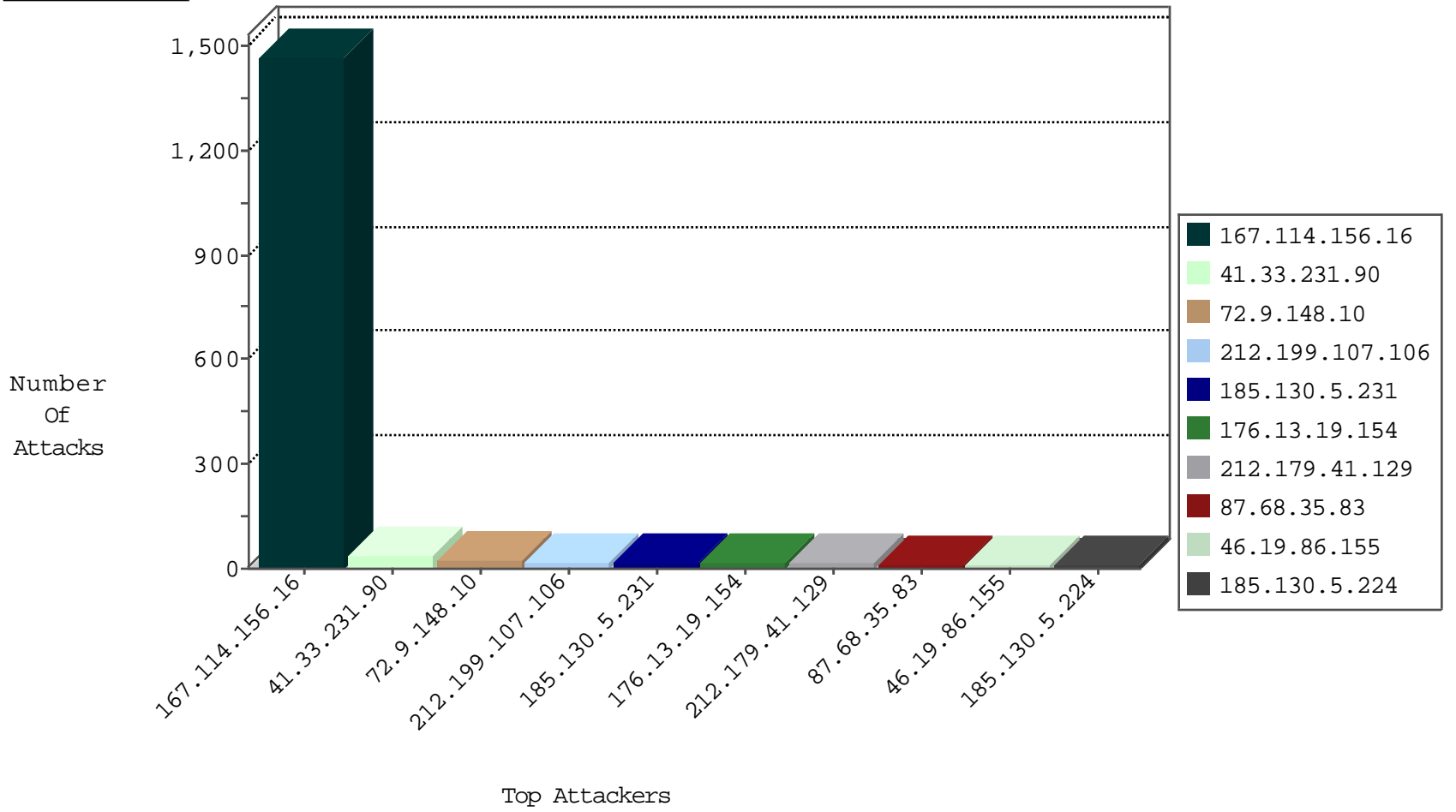
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3209
151.0.151.137	Romania	147.237.72.14	dover.idf.il(old)	I4 Source or Dest Port Zero	drop	4
74.91.124.204	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
123.195.116.221	Taiwan	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.31	nakchal.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.77.235	sviva.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.77.205	prisha.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	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
104.199.129.163	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP osCommerce categories.php Arbitrary File Upload And Code Execution	2
176.13.19.154	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
121.201.61.49	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.0.19	Austria	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.77.179	Korea, Republic of	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.39		mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.111.229	147.237.77.19	Philippines	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.64	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.77.179	Korea, Republic of	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.199.107.106	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
212.179.41.129	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
87.68.35.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.19.154	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
77.127.25.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.155	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.116.217.178	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.228.11.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.19.154	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.120.192.241	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.16.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.201.38	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.177.224.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.164.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.142.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.179.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.106	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.10.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.123.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.59	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.121.120.75	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.106	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
109.66.211.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
37.46.39.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.18.95	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.36	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.160	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
101.198.159.31	China	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.36.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.104	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.175	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.117.180.21	Luxembourg	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
109.186.190.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1
93.189.26.18	Austria	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
84.229.128.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
87.68.241.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
104.199.129.163	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
94.230.83.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
104.199.129.163	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 104.199.129.163	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19372-he/idfgdover.aspx	Block	1
46.19.86.155	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.58.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.159	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
141.212.122.160	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
104.199.129.163	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.199.129.163	Block	1
77.125.74.149	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 77.125.74.149 (sigalgs DoS Attack)	None	1
207.46.13.45	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1
66.249.66.63	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
52.90.147.148	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
176.12.141.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.3	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.3	Block	1
77.125.74.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
54.152.106.69	United States	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/./shared/clientscripts/scroller/jquery.jcarousel.js	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
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.16.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
104.199.129.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1524-en/admin/categories.php/login.php	Block	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
109.64.133.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
104.199.129.163	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	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
66.249.66.7	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.39.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19815-he/idfgdover.aspx	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/1/1431.pdf	Block	1
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1