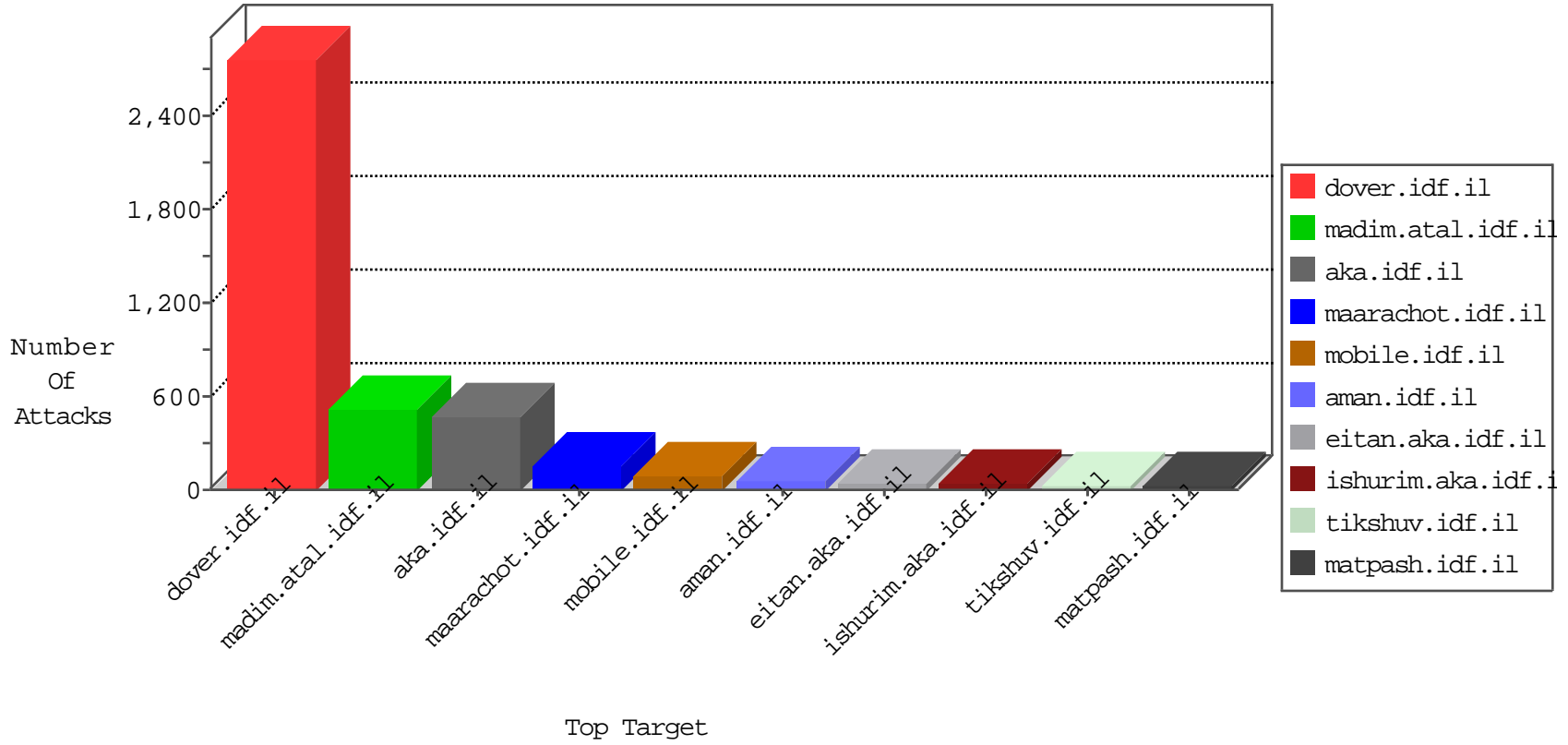


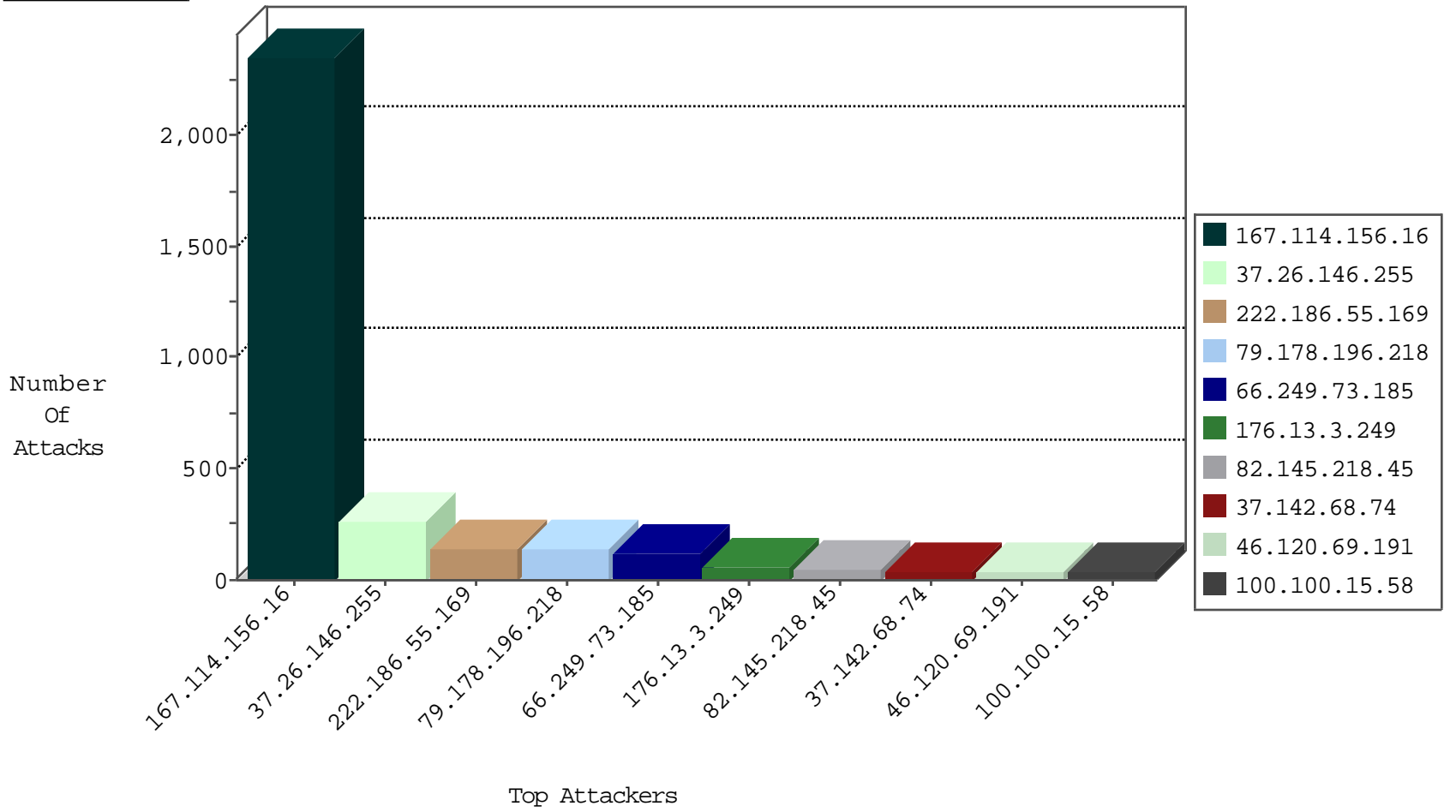
# IDF Under Attack Daily Report



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	3700
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
112.67.98.25	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
93.172.23.131	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
41.142.202.55	Morocco	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	2
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.19.85.24	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
87.69.26.123	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.142.202.55	147.237.77.216	Morocco	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
61.191.190.47	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
61.191.190.47	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.155	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.191.190.47	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.210	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
58.17.86.12	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.191.190.47	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.218	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP JBoss JMXInvokerServlet access attempt	1
61.191.190.47	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
125.66.55.157	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.191.190.47	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.191.190.47	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.210	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.210	147.237.0.16	Netherlands	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.191.190.47	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	118
222.186.55.169	China	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	108
82.145.218.45	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	43
222.186.55.169	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	36
100.100.15.58		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
100.100.34.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
100.100.85.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.19.85.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
46.120.152.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
213.57.133.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
46.19.85.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.120.126.32		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	12
46.19.86.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.6.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.120.126.37		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.106.189		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.109.26		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
77.125.124.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
176.13.22.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.197	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.207	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.163	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.83.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
100.100.4.180		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
100.100.24.200		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
5.22.134.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
172.56.16.105	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.34.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
188.120.148.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.210.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.41.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.75.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.14.74	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.30.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.145.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.91.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
79.178.196.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
79.178.196.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.13.3.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.120.69.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.69.191	Block	36
37.142.68.74	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.68.74	Block	36
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
176.13.7.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.6.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.120.69.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/69693.jpg	Block	4
31.210.186.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
46.19.85.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.33.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.52.160.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.92.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	2
2.54.8.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	2
84.111.137.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
46.19.86.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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	2
31.168.28.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.242.5.209	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
47.18.93.58	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.54.161.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.160.224.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.45	Block	1
91.135.102.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.169.22	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1134-he/dover.aspx	Block	1
185.3.146.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
84.228.97.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.116.140.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.112	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
31.154.92.180	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 31.154.92.180 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
80.246.136.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.28.179	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
212.199.57.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1