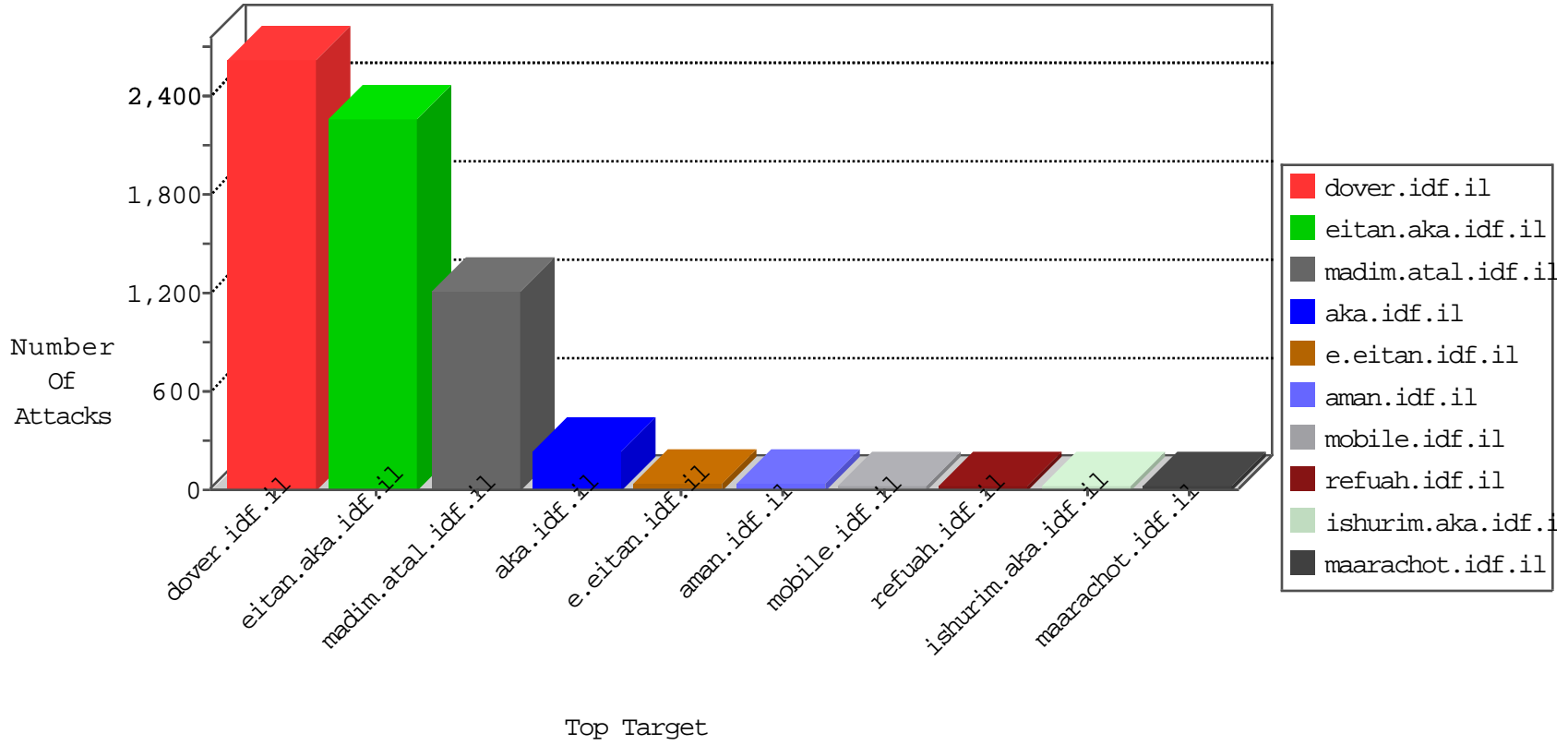


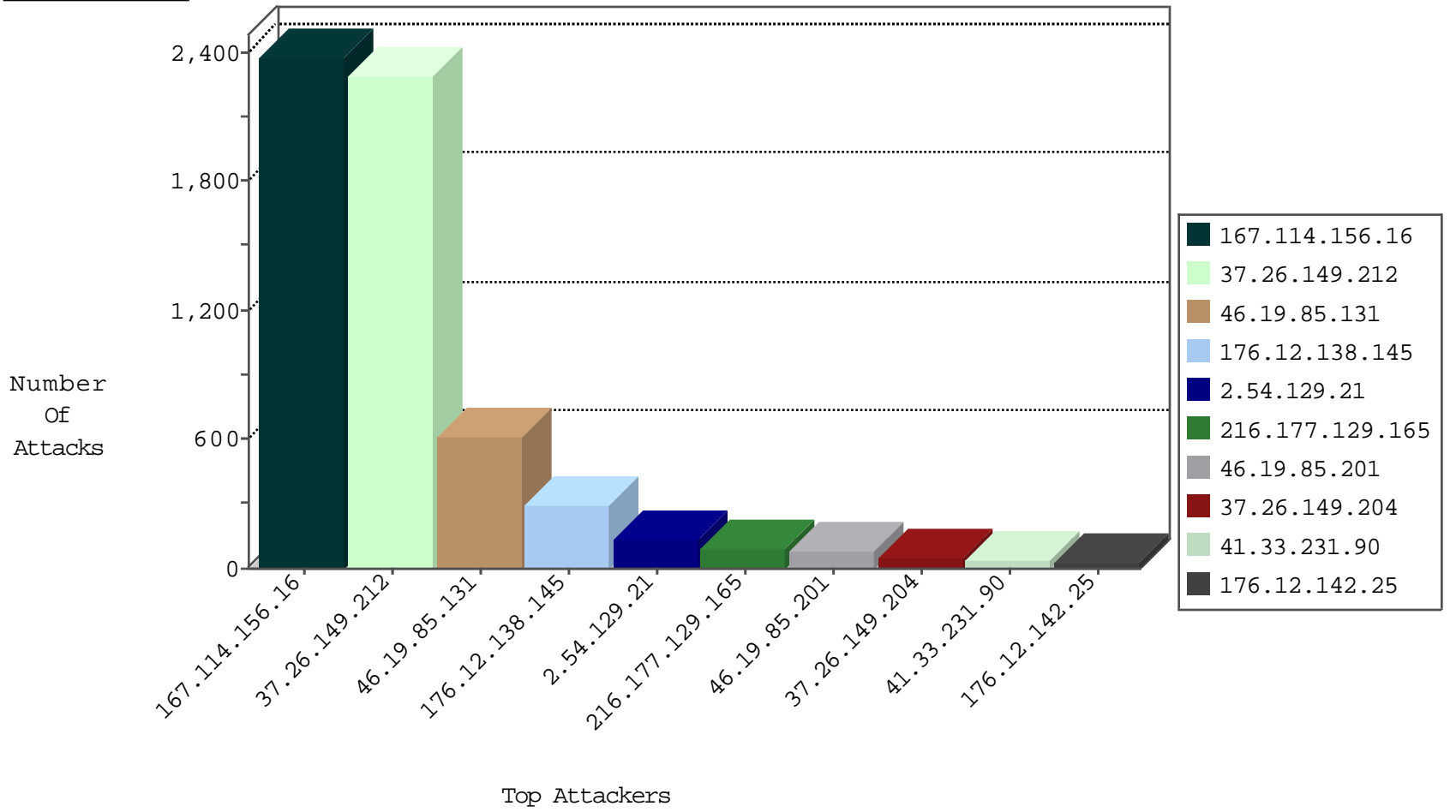
IDF Under Attack Daily Report



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	3502
37.26.146.154	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	122
216.177.129.165	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	58
66.249.69.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
178.57.216.17	Russian Federation	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	2
216.177.129.165	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.106.94.126		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
213.57.139.98	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
61.160.207.52	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	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
176.12.138.145	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
108.61.96.127	147.237.8.27	Australia	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
113.106.129.219	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.8.45	France	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.204	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
201.166.248.135	147.237.72.156	Mexico	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.109.112.72	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.106.129.219	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
85.143.220.201	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	312
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	131
216.177.129.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
2.54.129.21	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.149.212	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
109.67.52.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.212	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.0.197.217	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	11
94.226.170.12	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
94.226.170.12	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.195	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.189.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
94.230.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.125.144.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.136.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.152.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.156.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.2.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
76.190.244.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.3.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.195	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.78.201	United States	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
216.177.129.165	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
188.120.148.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.60.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.146.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.201	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	3
80.246.139.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
2.54.156.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.57.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.168.206.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.25	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.147.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.218.34	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.212	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1928
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	295
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	258
176.12.138.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
176.12.138.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.129.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
176.12.138.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	56
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
46.19.85.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	54
37.26.149.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
176.12.142.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	16
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
58.248.103.201	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
176.13.8.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
58.248.103.201	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 58.248.103.201	Block	3
2.52.58.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.65.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.83	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
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
176.12.150.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
79.182.15.84	Israel	147.237.0.19	madim.atal.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/1133-22638-he/dover.aspx.	Block	2
84.229.63.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.185.168	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.126.215.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
58.248.103.201	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/plus/download.php	Block	2
95.86.68.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
46.117.212.144	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Double URL Encoding	Block	1
81.218.162.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
31.168.239.231	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
176.13.7.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.210.188.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.67.121.131	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.68.65.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.201	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
79.180.8.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.149.212	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/404.aspx	Block	1
185.27.105.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.97.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.84	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/news/null	Block	1
95.86.96.19	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucNewsFlashControl\$txtSearch in www.idf.il/1153-he/dover.aspx	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
84.108.12.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.172	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.146.173	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1