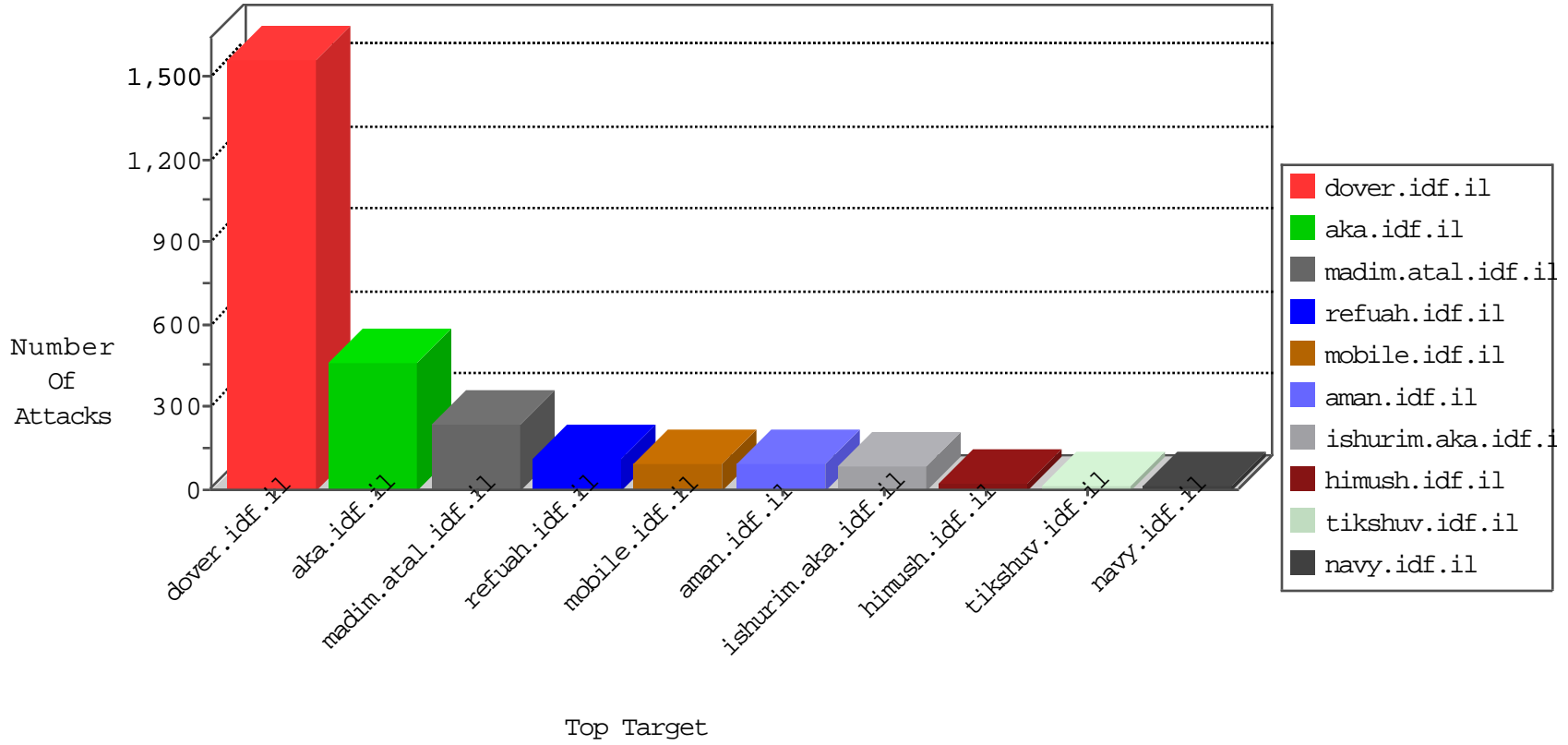


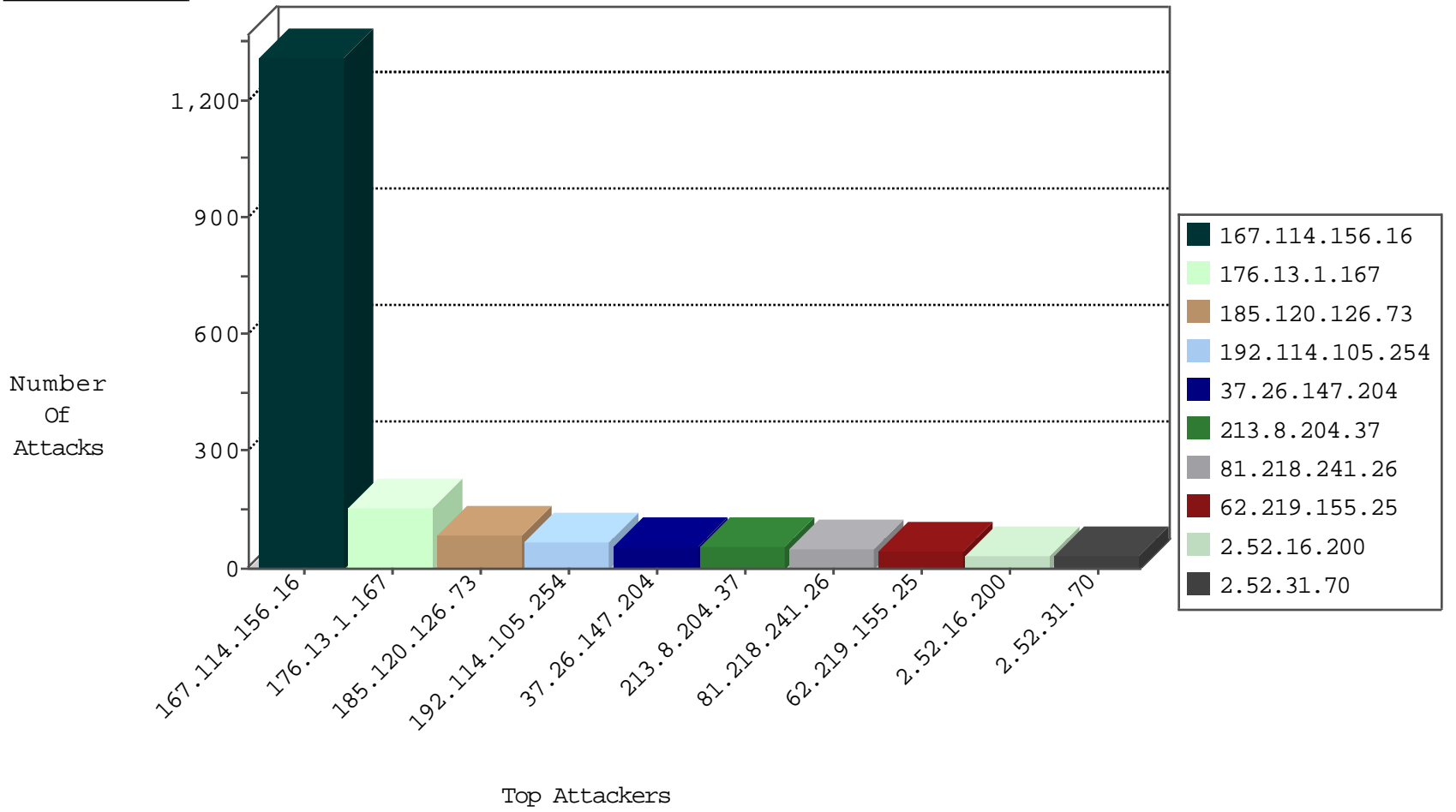
# IDF Under Attack Daily Report



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	3049
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	406
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	350
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	276
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
207.46.13.75	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.133.226	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
212.25.121.195	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.40	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
183.40.128.33	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

01-06-2016-11:04:01 to 01-06-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.25.105.125	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
64.183.83.122	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1
64.183.83.122	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
46.165.222.227	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.229	147.237.72.166	Israel	aka.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
106.75.199.201	147.237.77.176	China	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
89.248.162.131	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.216	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
64.183.83.122	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
64.183.83.122	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
46.165.222.227	147.237.76.148	Germany	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.203	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.35.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.183.83.122	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	67
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
213.8.204.37	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
62.219.155.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
2.52.16.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.52.175.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
107.167.104.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.176.13.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
2.54.13.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.49.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.210.166.181	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
2.52.31.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.52.31.70	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.31.70	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.31.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.31.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.110	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.146.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.163.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.96.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.136.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.180.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.96.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.32.179.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.178.0.113	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
199.203.62.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
147.235.185.74	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.158.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.158.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
112.111.161.190	China	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.144	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.202.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
157.55.2.139	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.0.252.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.117.96.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.21.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.212.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.96.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
43.255.176.89	Japan	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
176.13.1.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
37.26.147.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
176.13.1.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
37.26.146.244	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.26.146.244	Block	22
109.253.219.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.52.16.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	7
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.8.194	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	4
112.111.161.190	China	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 112.111.161.190	Block	4
80.246.139.215	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
213.8.204.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
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	3
79.176.96.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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	3
2.54.40.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
89.139.154.197	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	3
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.223.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.170	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	2
46.19.86.25	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
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	2
89.138.46.119	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	2
79.178.49.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
176.13.20.220	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	2
2.54.40.254	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
65.132.59.34	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	2
95.35.37.225	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1669-he/refuah.aspx	Block	2
109.253.143.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.204.238	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	2
176.13.22.60	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	2
95.86.86.254	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
79.181.59.69	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.147.17	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
37.26.147.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
66.249.93.105	Israel	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on www.chimush.atal.idf.il/994-8447-he/himush.aspx*x@x"	Block	1
176.13.15.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.11.63	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.0.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
62.219.137.44	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.213.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.25.105.125	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1