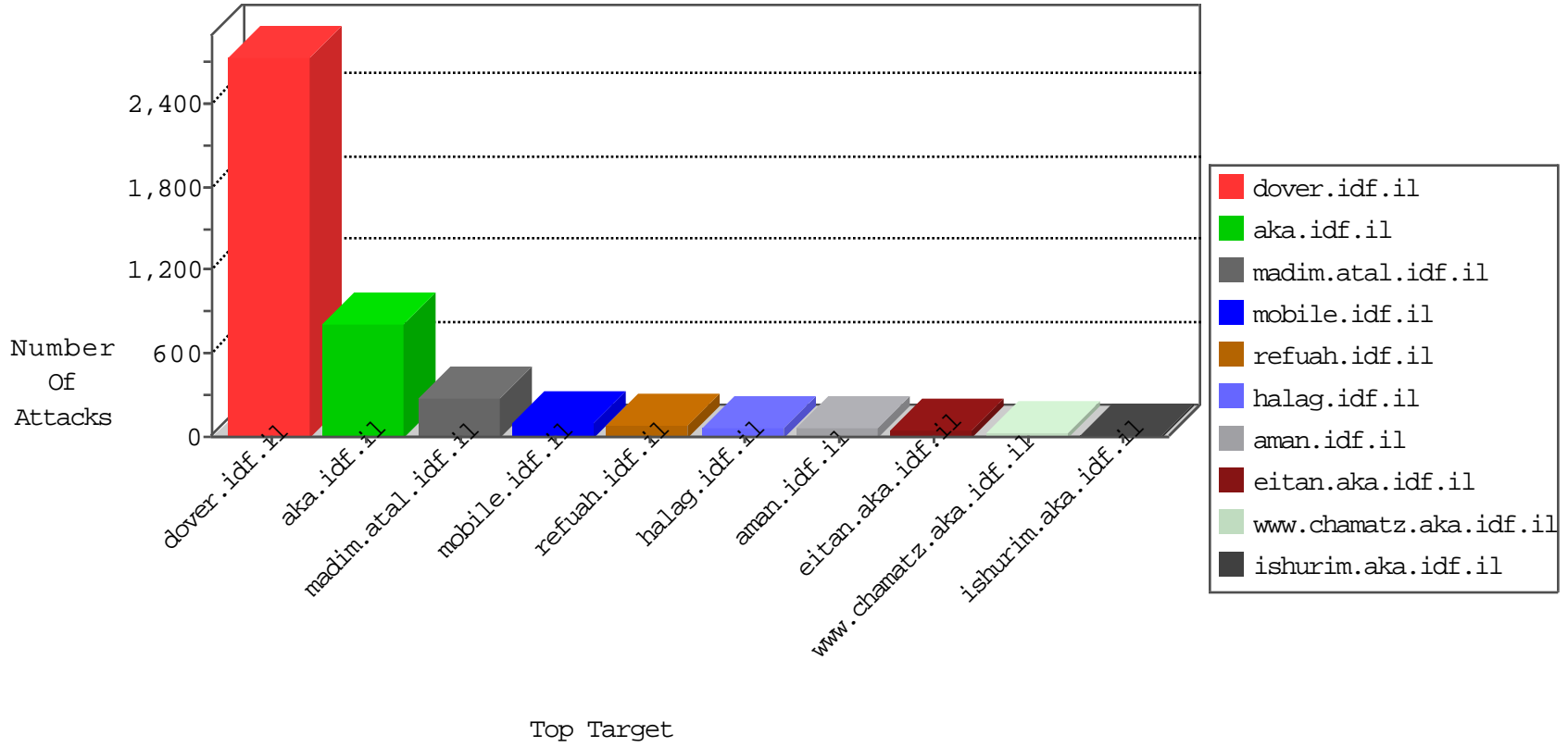


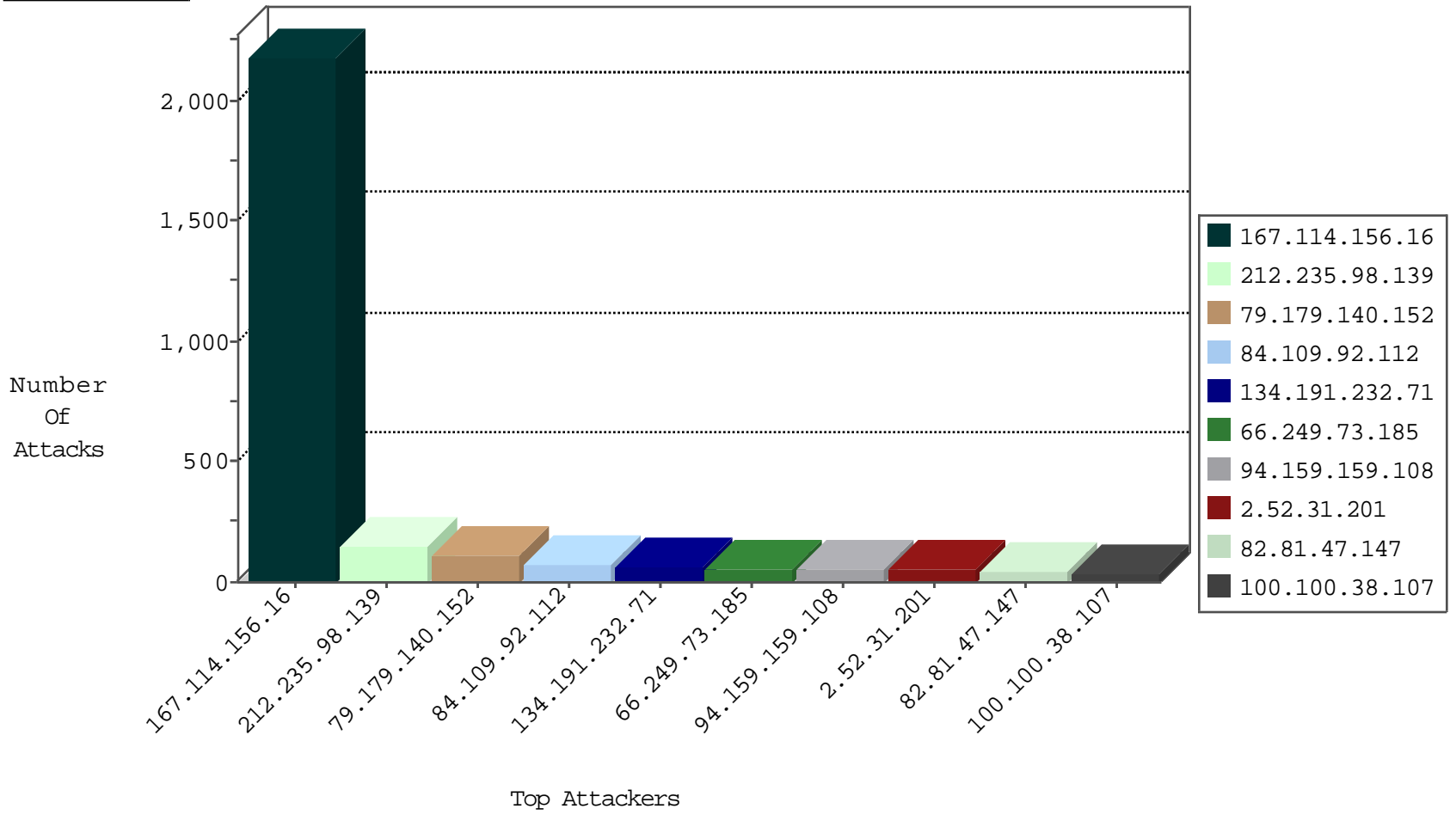
# IDF Under Attack Daily Report



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	3365
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	15
23.95.248.132	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
62.209.11.138	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
23.95.248.132	United States	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1
62.209.11.136	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
95.213.128.110	Russian Federation	147.237.77.234	halag.idf.il	L4 Source or Dest Port Zero	drop	1
62.209.11.137	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.105.199.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.134	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.37.208	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
84.94.200.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.103.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.43.113.24	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.18.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.56.80.31	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.77.235	Poland	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.43.236.38	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
95.86.68.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.228.144.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
188.120.148.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.63.243.41	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.67.138.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.174.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.120.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.27.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
90.43.151.166	147.237.77.226	France	www.chamatz.aka.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
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	120
84.109.92.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
2.54.138.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
77.125.90.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
100.100.116.202		147.237.72.166	aka.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	28
100.100.8.168		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
212.150.66.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
94.159.159.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
94.159.159.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
107.167.99.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
2.52.31.201	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
2.52.31.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.49.116		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.32.148		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
124.179.64.49	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.32.148		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.107.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.94.208.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
100.100.38.107		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.38.107		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.38.107		147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.63.240		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.9.181		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.13.4.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.83.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.39.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.107.242		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
176.13.9.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.143.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
199.203.226.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.162	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.82.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
192.115.177.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.235.98.139	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.8.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.82.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
79.182.202.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.102	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.202.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.140.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
82.81.47.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
79.180.125.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.13.18.53	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	33
80.246.137.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
212.235.98.139	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.235.98.139	Block	23
80.246.136.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.54.14.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
80.246.140.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
2.54.9.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
77.75.76.170	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.75.76.170	Block	5
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.61	Block	5
79.178.151.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
5.9.73.213	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.9.73.213	Block	4
109.186.185.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
80.246.139.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.3.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.142.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
84.109.233.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.150.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.40.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
109.65.175.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
85.64.227.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
79.179.140.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
176.12.143.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.127.196.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.4.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
83.130.118.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyius/controls/atuda/Å	Block	2
77.125.95.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
185.32.179.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.10.209	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	2
176.12.140.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.216.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.154.9.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
132.74.58.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/110417.pdf	Block	2
79.183.171.102	Israel	147.237.72.166	aka.idf.il	Too Many 403: Response Code per Session	Block	1
188.25.238.171	Romania	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/5/1695.pdf	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
46.120.32.116	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/gyius/miyun/miyunprocessquestionnaire.aspx	None	1
176.13.3.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.214.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
150.70.173.9	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.142.162.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.140.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.191.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.36.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1