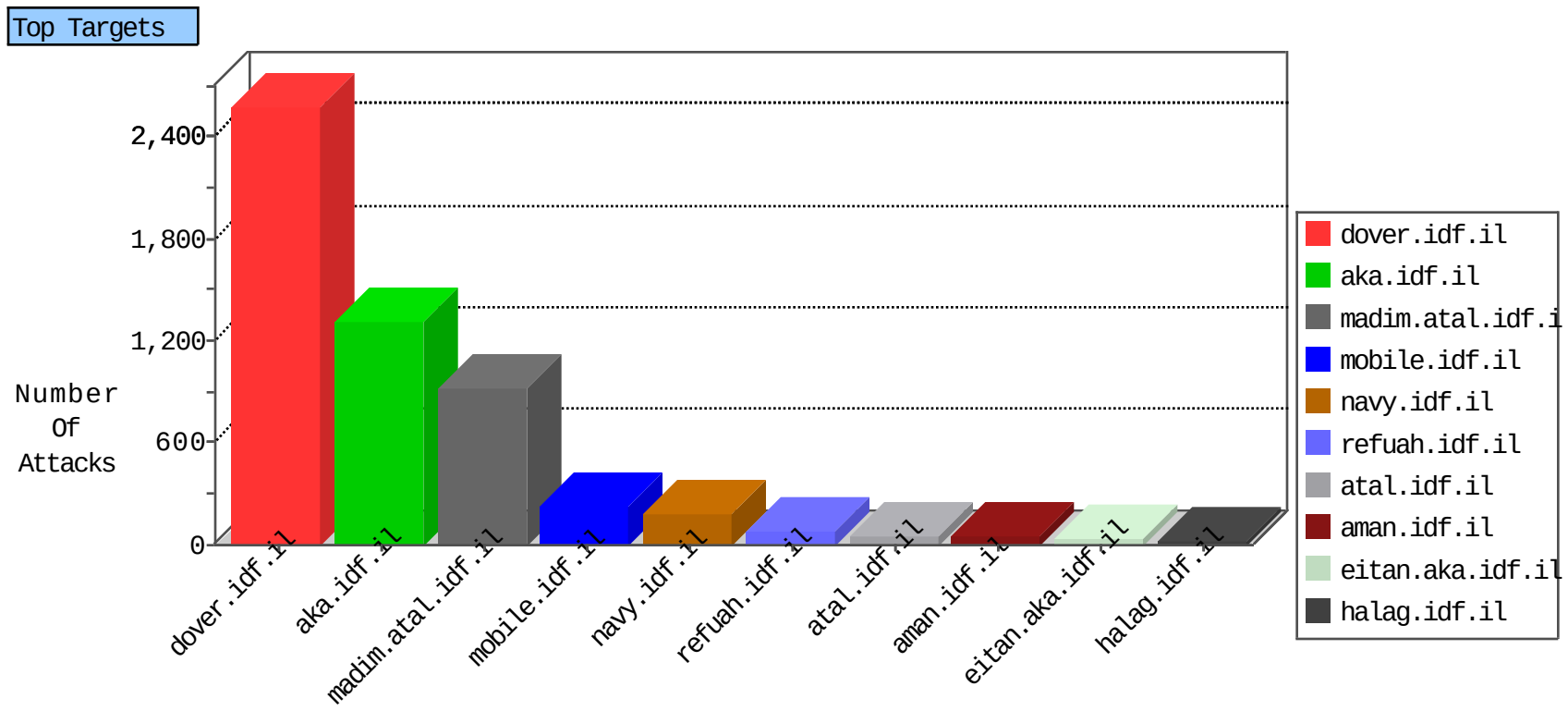
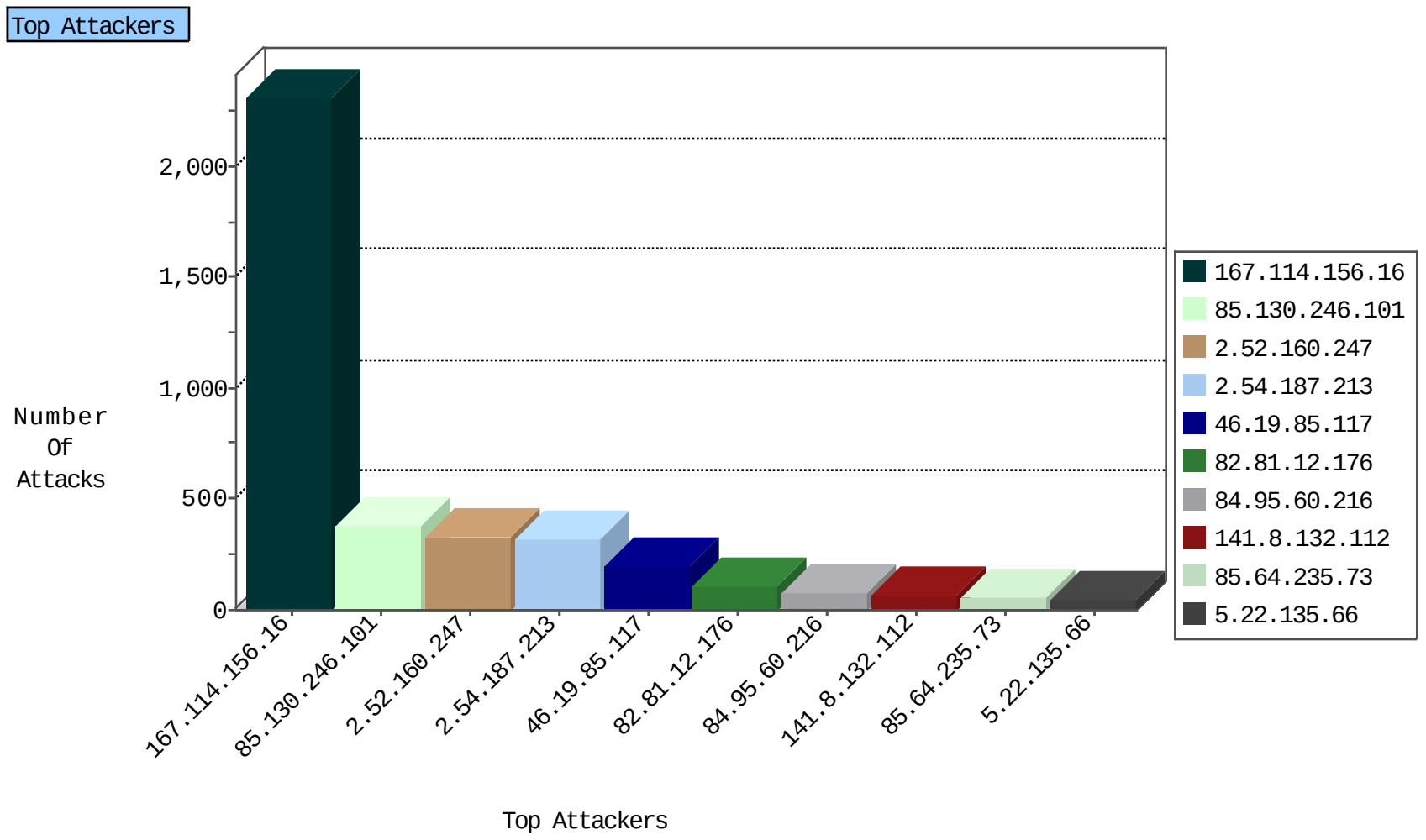
01-24-2016-16:04:08 to 01-24-2016-17:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-24-2016-16:04:08 to 01-24-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3213
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3083
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-24-2016-16:04:08 to 01-24-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.218.36.252	Taiwan	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	2

01-24-2016-16:04:08 to 01-24-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.32.179.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.138.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.93.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.62.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.109.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
191.240.136.5	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.13.173	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.148.90	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
5.29.97.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-24-2016-16:04:08 to 01-24-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.246.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	372
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
85.64.235.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
5.22.135.66	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
84.95.60.216	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	37
185.89.217.230		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
109.67.163.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
185.89.217.235		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
216.185.39.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
107.167.105.159	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
107.167.109.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
85.65.19.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
80.179.114.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.54.166.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
80.179.114.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.232		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.225		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
185.89.217.227		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
185.89.217.233		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
85.250.246.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.14.64	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.231		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
37.26.149.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.250.246.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
85.64.235.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
185.89.217.229		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
46.19.86.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.166.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.48.37	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	9
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.89.217.226		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
94.230.86.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.89.217.228		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
82.166.247.98	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
87.69.135.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.246.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.176.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.22.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.50.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.45.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.193.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.10.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.148.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.187.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	193
2.52.160.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	139
2.52.160.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.54.187.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	97
2.52.160.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	55
84.95.60.216	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	31
46.19.86.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
2.54.138.249	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	19
79.181.51.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.51.191	Block	17
80.246.136.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
213.8.128.96	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 213.8.128.96	Block	14
46.19.86.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
2.54.187.213	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.187.213	Block	12
46.19.86.212	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	9
79.180.163.149	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.163.149	Block	7
79.179.122.158	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
109.253.215.112	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.4.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.139.2	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
37.26.147.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.139.2	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
176.13.11.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.135.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
109.253.192.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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	2
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.10.179	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
84.95.60.216	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	2
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
37.142.68.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.32.252	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers from 2.52.32.252	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
157.55.39.171	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.171	Block	2
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.228.176.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.136.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.22.130.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.126.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
158.69.109.58	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
46.19.86.78	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
91.135.111.85	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1