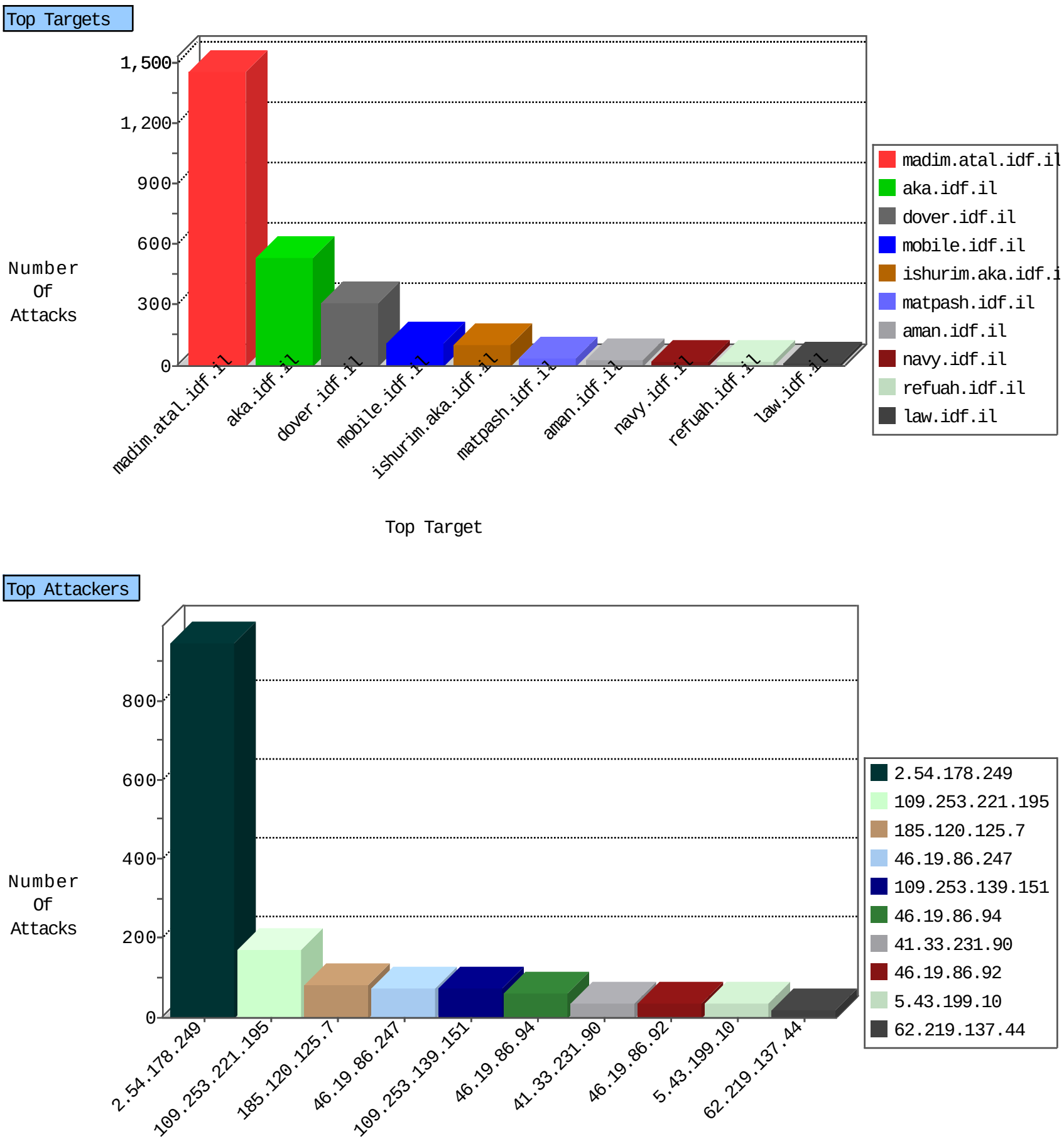
02-01-2016-10:04:10 to 02-01-2016-11:04:10

IDF Under Attack
Daily Report



02-01-2016-10:04:10 to 02-01-2016-11:04:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
93.115.97.116	Romania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
93.115.97.116	Romania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
95.100.174.66	Europe	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-01-2016-10:04:10 to 02-01-2016-11:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.87.46.138	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
52.26.202.58	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
91.121.60.119	France	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-01-2016-10:04:10 to 02-01-2016-11:04:10

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.196.59.34	147.237.76.177	Chile	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
37.26.149.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.196.59.34	147.237.0.35	Chile	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.179	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
85.130.240.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.209.224	147.237.77.216	Israel	dover.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
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.150.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.235.135.88	147.237.77.216	Lebanon	dover.idf.il	ET SCAN NMAP -sA (2)	1
190.196.59.34	147.237.77.233	Chile	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
190.196.59.34	147.237.8.14	Chile	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.0.15	Chile	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.233.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.166.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.213.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.163.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.96.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.196.59.34	147.237.77.74	Chile	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
190.196.59.34	147.237.8.27	Chile	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-01-2016-10:04:10 to 02-01-2016-11:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.43.199.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	34
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.177	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
37.142.156.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.178.249	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.140.148	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.179.10.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.154	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.46.39.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
80.246.138.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.148.147	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.143.87.230	United Kingdom	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.166.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.126.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.201.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.173.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.25.91.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.210.178.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.203.147	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.107	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.145.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.198.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.15.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.251.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.253.201.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.109	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.201.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.243	Israel	147.237.77.216	dover.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
46.19.86.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.184.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-01-2016-10:04:10 to 02-01-2016-11:04:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.178.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	671
2.54.178.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	264
109.253.221.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
109.253.139.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
109.253.221.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
2.52.130.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
79.183.140.71	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.183.140.71	Block	17
109.253.139.146	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	14
176.13.7.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
176.13.23.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.23.105	Block	12
2.54.149.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.180.112.10	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	6
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.48.21	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.48.21	Block	4
37.26.149.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.133.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.133.72	Block	3
46.19.85.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	3
2.54.177.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	3
109.253.216.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.43.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.150.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
2.54.48.21	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
91.121.60.119	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.121.60.119	Block	2
109.253.210.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter SearchParam in www.aka.idf.il/main/sachar/	None	2
176.13.23.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
2.54.136.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
91.121.60.119	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
80.246.133.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/×'×™××•×¡	Block	2
109.253.136.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.97.13.226	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
2.54.177.53	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.177.53	Block	2
87.68.166.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.15.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
176.13.20.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.217.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.197.89	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
2.54.46.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.26.210	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.52.135.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

02-01-2016-10:04:10 to 02-01-2016-11:04:10