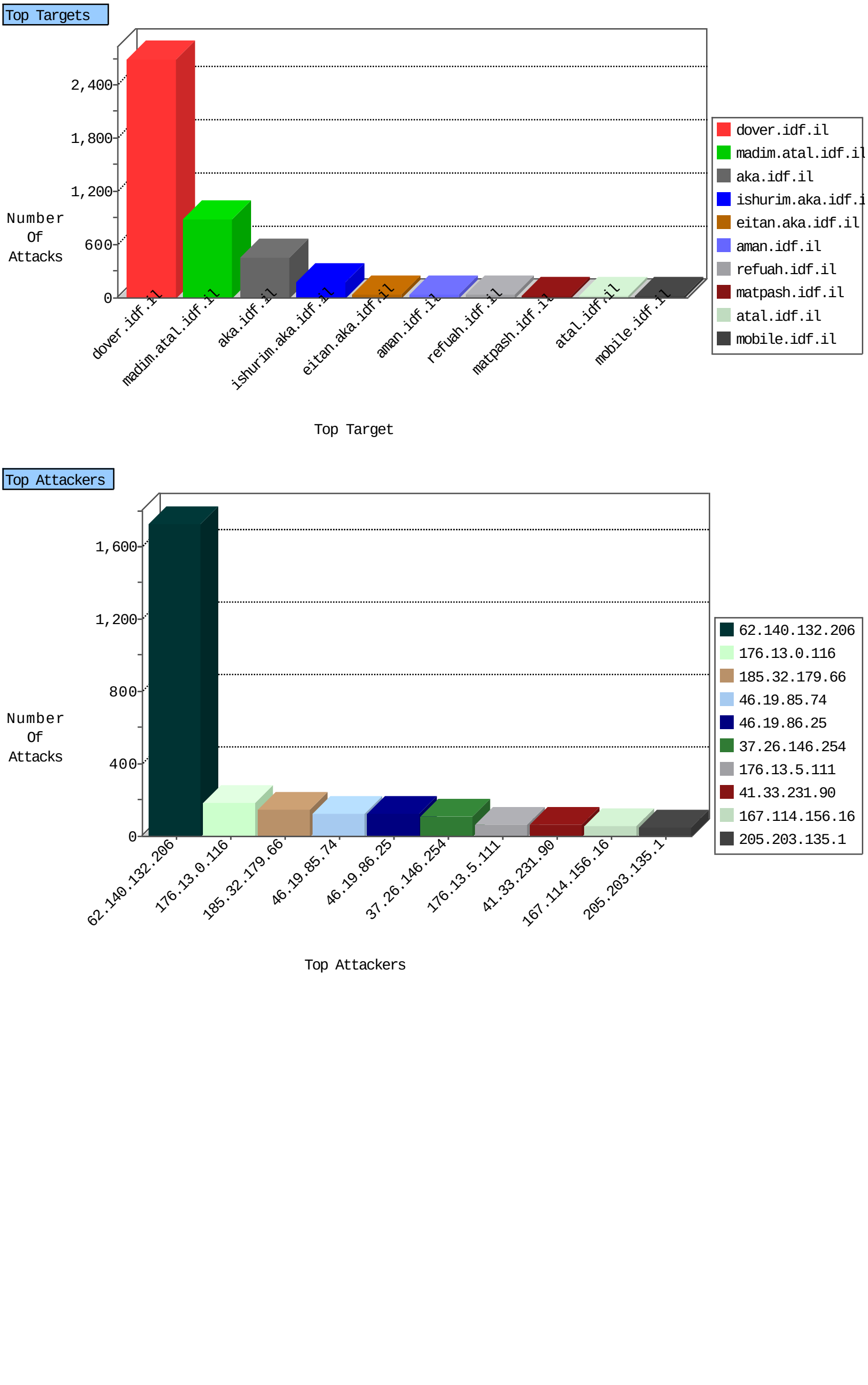
11-24-2015-09:04:07 to 11-24-2015-10:04:07

IDF Under Attack
Daily Report



11-24-2015-09:04:07 to 11-24-2015-10:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	1340
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
82.80.89.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

11-24-2015-09:04:07 to 11-24-2015-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.162.114	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
151.80.31.142	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.28.162.51	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-24-2015-09:04:07 to 11-24-2015-10:04:07

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	2
63.142.161.5	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.246.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.68.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.135.12	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	1
183.61.109.189	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
104.243.16.124	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
87.69.217.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.149	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.76.38	Poland	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.58.102.125	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
192.198.151.37	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
185.120.126.7	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -f -sS	1
94.102.60.175	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.137.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-24-2015-09:04:07 to 11-24-2015-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.140.132.206	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1725
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	126
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.60.34.247	Palestinian Territory, Occupied	147.237.77.216	dover.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	27
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.63.15		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
169.53.189.7	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
77.158.88.41	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.148.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.182.127.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
122.52.181.174	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
219.149.55.242	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.232	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	11
2.54.19.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
112.198.90.33	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
131.253.25.161	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.22.134.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.47.82	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.201.170.199	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.198.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.133.226	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.66.107	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
69.31.51.140	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.79.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
183.79.219.165	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
193.106.52.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
158.116.192.2	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

11-24-2015-09:04:07 to 11-24-2015-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
176.13.0.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
37.26.146.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
176.13.5.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
176.13.11.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
89.138.213.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
185.32.179.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
109.66.187.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
37.26.146.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	22
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	21
176.13.5.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
2.52.167.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.12.147.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.64.55.7	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
212.179.93.98	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
5.102.229.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.41.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
192.116.213.210	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.116.213.210	Block	5
192.116.213.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	5
109.66.187.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
176.13.11.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.0.101.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	3
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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	2
2.54.146.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.20.209.217	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	2
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.134.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.117.171.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
176.13.2.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.138.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.120.115.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.32.128	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
37.26.148.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1

11-24-2015-09:04:07 to 11-24-2015-10:04:07