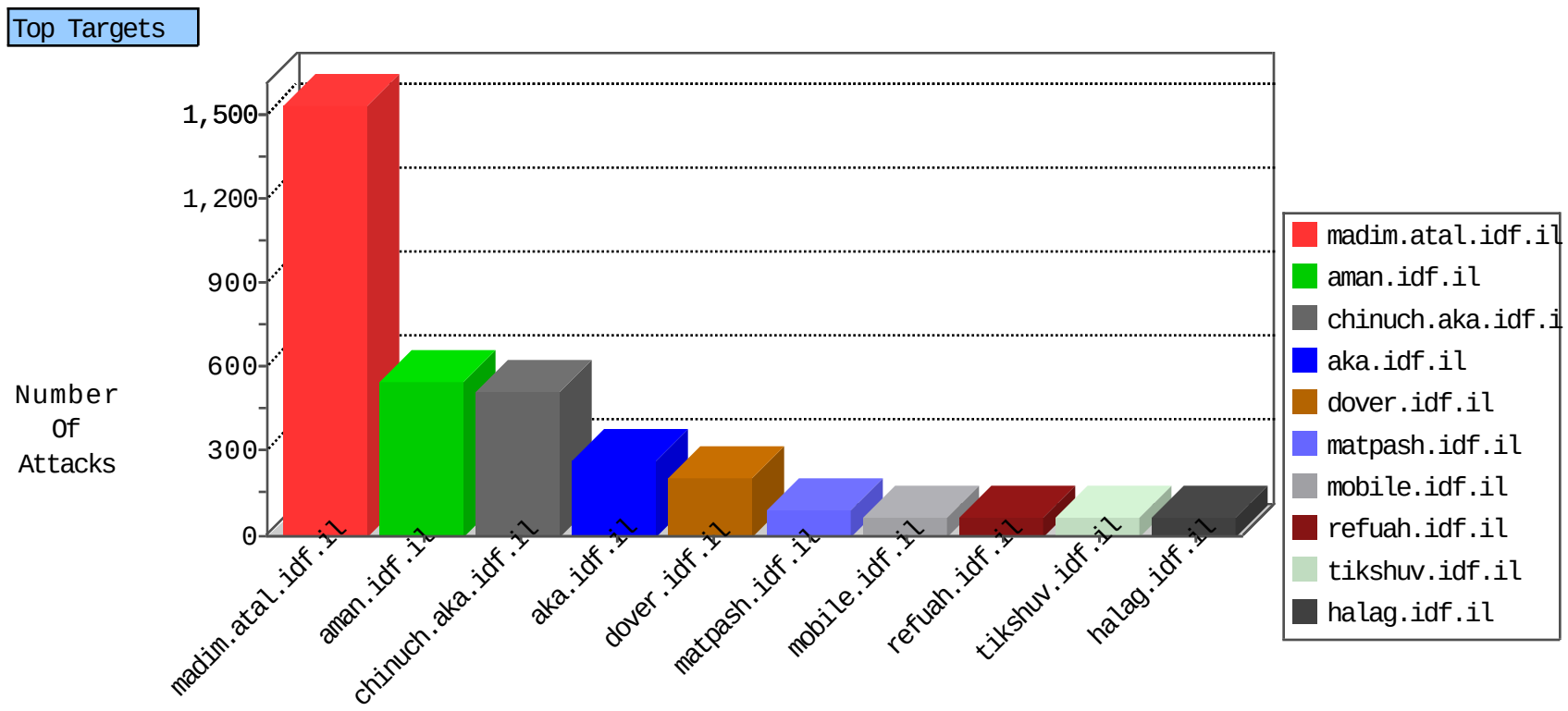
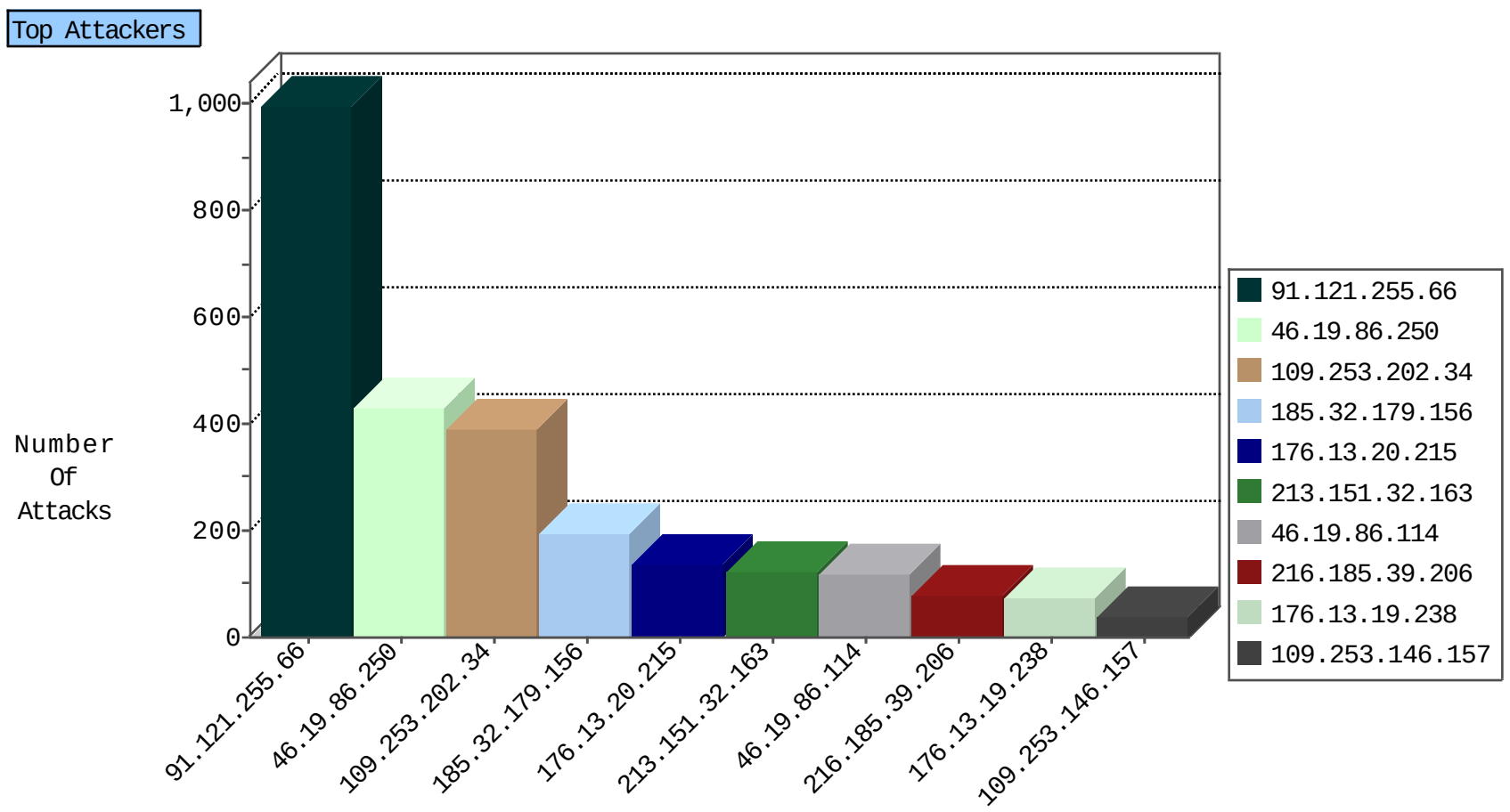
01-27-2016-14:04:03 to 01-27-2016-15:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-27-2016-14:04:03 to 01-27-2016-15:04:03

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	1535
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
109.65.159.54	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
61.160.224.129	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-27-2016-14:04:03 to 01-27-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.149.18.250	United States	147.237.76.147	chinuch.aka.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-27-2016-14:04:03 to 01-27-2016-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.250.57.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.227.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.255.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.169.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.88.129.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.204.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.239.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.20.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.181.145.71	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.22.134.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.177.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
149.78.165.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-27-2016-14:04:03 to 01-27-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	493
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	367
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	111
216.185.39.206	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	76
109.253.146.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
109.253.204.113	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
109.66.34.241	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.85.17	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
93.173.191.121	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
80.246.130.163	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.34.12.47	Jordan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
79.177.10.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.172.18.44	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
80.246.130.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.45.231	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.56.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
93.173.8.212	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
154.117.129.10		147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	9
213.55.114.225	Ethiopia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
66.249.81.196	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.187	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.238.136.21	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.126	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.126	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.21.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.183.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.148.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
84.108.250.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.148.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.45.231	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.188.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.187	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.45.231	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.45.231	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

01-27-2016-14:04:03 to 01-27-2016-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.202.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	259
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	258
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
185.32.179.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.202.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
185.32.179.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
176.13.20.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.13.19.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
176.13.20.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
109.253.202.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	30
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
176.13.17.83	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
84.108.139.188	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.139.188	Block	10
176.13.15.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
87.69.127.143	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	7
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.253.130.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
109.253.198.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.148	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.69.127.143	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.69.127.143	Block	6
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.194.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.44.129.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/&sa=u&ved=0ahukewiazsb2_8nkahvlaxokhznpal0qfgghmaa&usg=afqjcneeywysowwcocycbntx0qxav9lbkw	Block	5
79.177.238.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
37.26.149.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
216.130.161.119	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.130.161.119	Block	3
176.13.18.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** *******, Observed ********** ********** ********** *	None	3
178.62.50.240	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
185.32.179.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.188.26	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
109.253.198.220	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
185.32.179.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	2
176.13.22.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.152.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.232.46.209	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 207.232.46.209	Block	2
37.142.64.7	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	2
93.143.91.241	Croatia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
2.54.40.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.83	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/officesmap/pages/aza.aspx	Block	1
46.19.85.249	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected C3AFF93D, Observed DD15DB9C	None	1

01-27-2016-14:04:03 to 01-27-2016-15:04:03