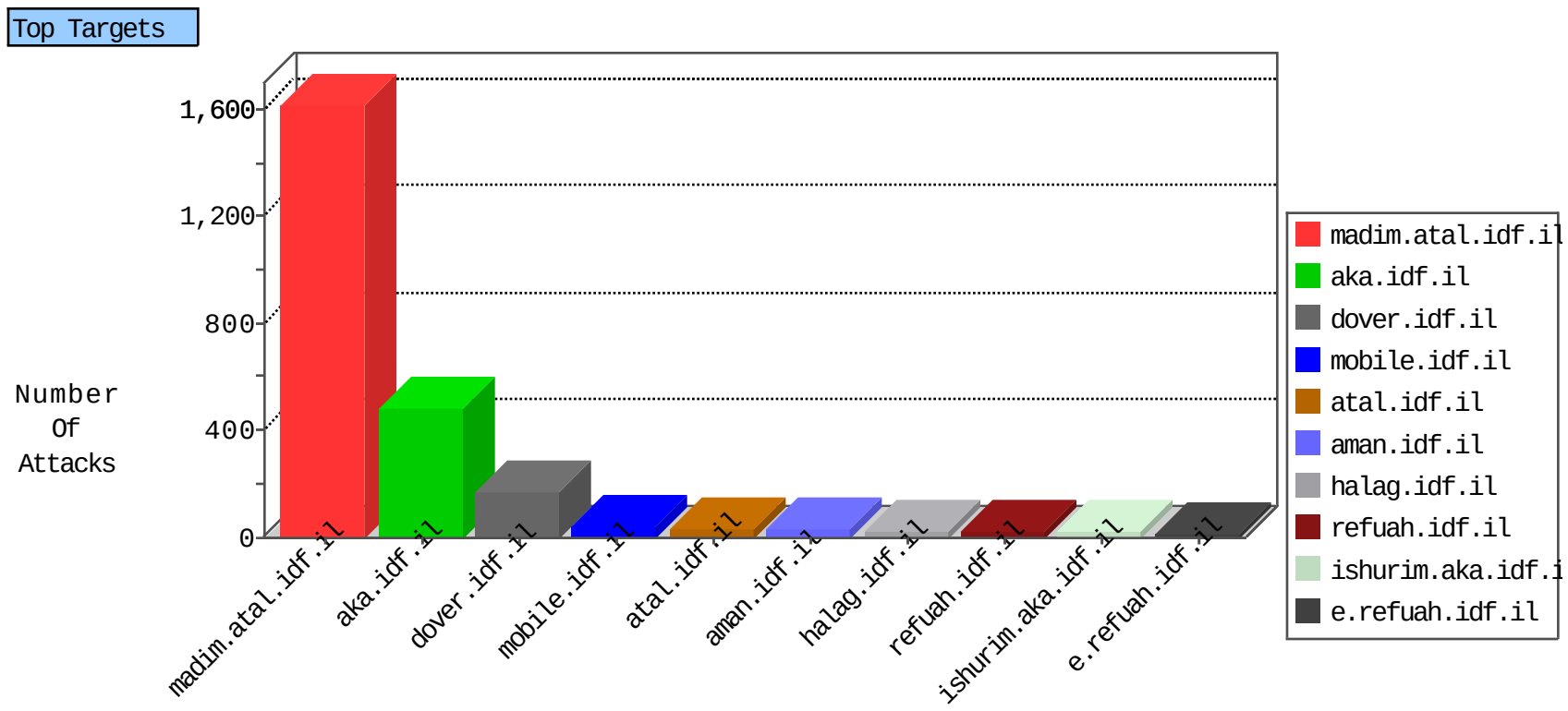
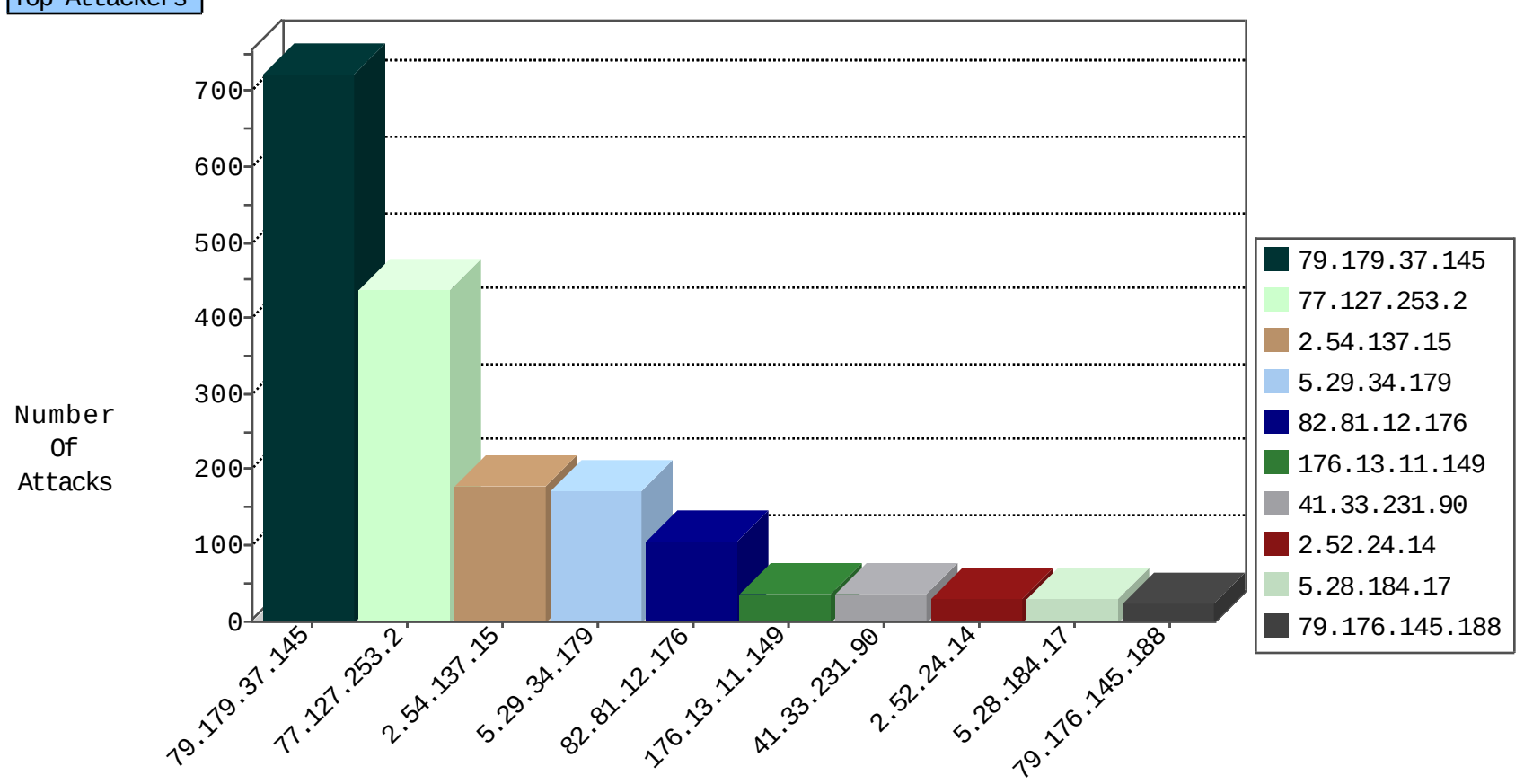
01-30-2016-18:04:08 to 01-30-2016-19:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-30-2016-18:04:08 to 01-30-2016-19:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	106
85.100.43.88	Turkey	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
85.100.43.88	Turkey	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
113.12.31.207	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-18:04:08 to 01-30-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-30-2016-18:04:08 to 01-30-2016-19:04:08

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	4
190.196.59.34	147.237.77.179	Chile	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
190.196.59.34	147.237.77.74	Chile	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
5.39.222.253	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.59.34	147.237.76.202	Chile	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.76.148	Chile	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.8.50	Chile	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.76.38	Chile	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.8.27	Chile	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.72.217	Chile	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.0.19	Chile	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.14.233.163	147.237.76.42	Italy	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.54.78.123	147.237.0.15	Chile	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
158.130.6.191	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
190.196.59.34	147.237.77.226	Chile	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.121.137.5	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN NMAP -sS window 4096	1
190.196.59.34	147.237.77.205	Chile	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.249.106.23	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.24.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.196.59.34	147.237.76.201	Chile	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.59.34	147.237.76.42	Chile	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.76.30	Chile	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.59.34	147.237.72.167	Chile	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.54.78.123	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
158.130.6.191	147.237.77.176	United States	matpash.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
125.26.114.161	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.196.59.34	147.237.77.216	Chile	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.35.69.237	147.237.76.42	Israel	refuah.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

01-30-2016-18:04:08 to 01-30-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.78.22.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.238	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	14
79.176.145.188	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
79.178.241.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.24.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
95.32.196.49	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.145.188	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	10
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
5.28.184.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.28.184.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
149.88.96.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.24.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.196.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.174.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.24.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.183.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.6.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.25.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.24.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.119.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.28.184.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.57.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.186.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.244.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
5.28.184.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.22.131.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.244.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
31.210.187.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.28.184.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.155.135	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.136	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
84.108.155.135	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.15.100	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4

01-30-2016-18:04:08 to 01-30-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.37.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	396
79.179.37.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.179.37.145	Block	220
77.127.253.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
77.127.253.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
5.29.34.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.54.137.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
79.179.37.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
77.127.253.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	75
2.54.137.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
5.29.34.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.13.11.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.66.52.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.148.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.64.195.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	4
84.109.12.128	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
109.253.133.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.201.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.48.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 87.69.48.54	None	3
176.13.18.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.137.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
89.138.71.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.181.137.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.146.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.250.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.109.38	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
46.121.214.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.8.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.143.56	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
79.182.233.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
84.108.116.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.173.180	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.81.10.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.251.27.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
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	1
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.182.64.11	Block	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
84.108.116.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
80.230.25.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
67.19.79.218	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
79.182.64.11	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.182.64.11	Block	1
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.0.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-30-2016-18:04:08 to 01-30-2016-19:04:08