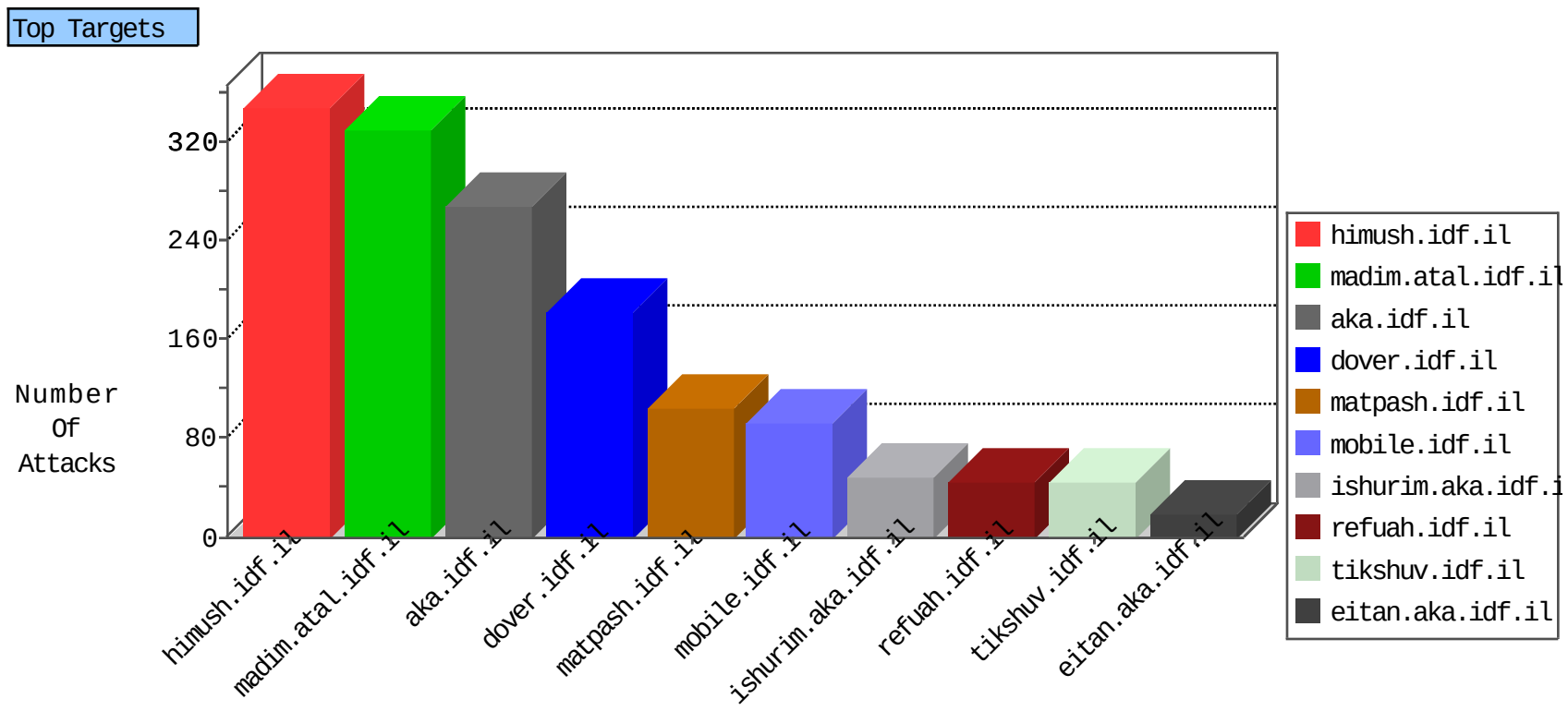
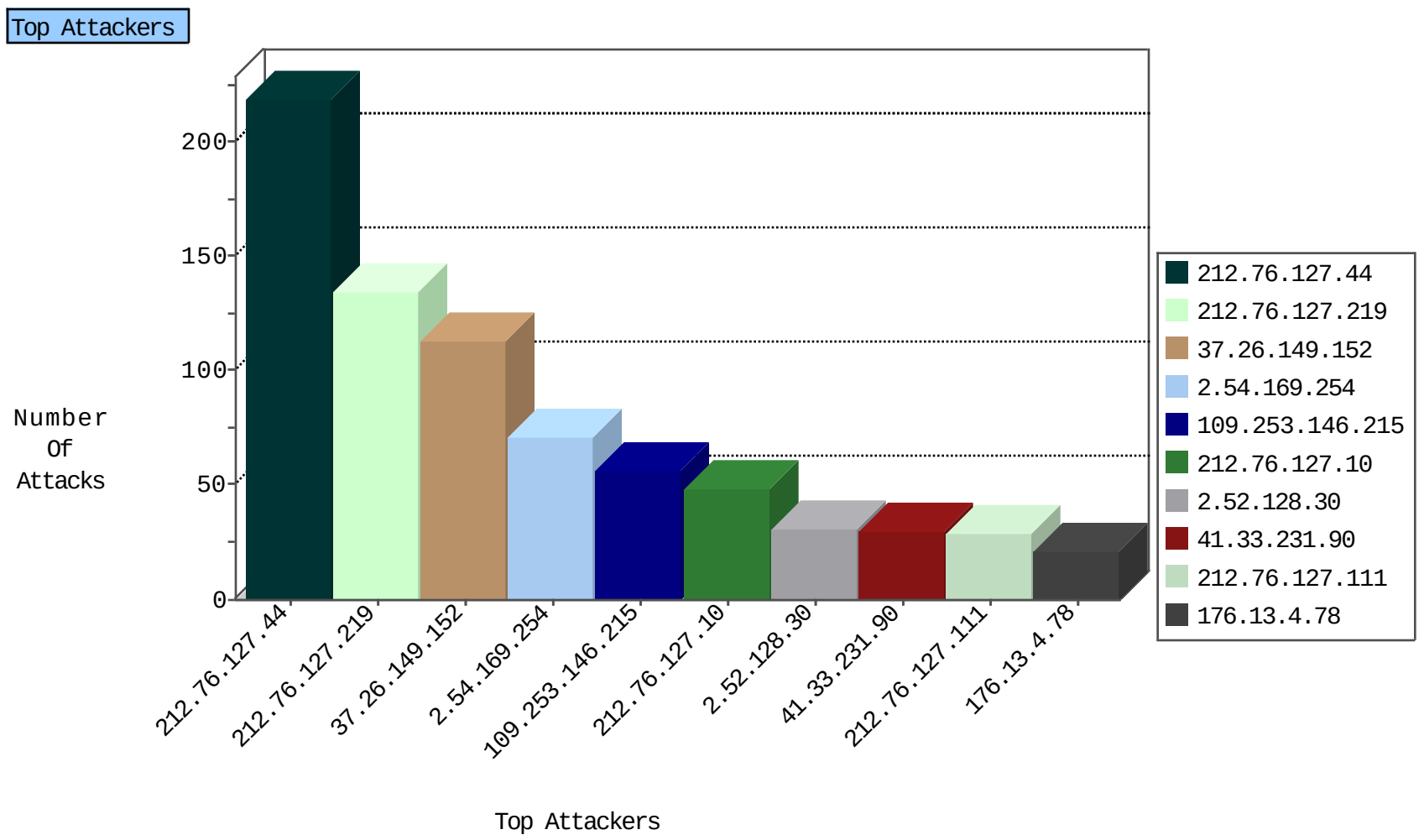
02-28-2016-08:04:00 to 02-28-2016-09:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-08:04:00 to 02-28-2016-09:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.140.167.188	China	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	4
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	2
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	1
184.105.247.235	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.239	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
109.236.93.206	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.103	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.199	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.247	United States	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
109.236.93.206	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.211	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1

02-28-2016-08:04:00 to 02-28-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.179.114.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
2.54.145.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
62.159.77.167	Europe	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
185.106.92.164		147.237.77.233	atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

02-28-2016-08:04:00 to 02-28-2016-09:04:00

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
46.117.181.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
136.0.99.20	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.227.71.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.103.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.89.71.130	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
213.8.7.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.212.109.229	147.237.0.19	Turkey	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.157.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.37.12.200	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.75.223	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
176.13.22.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.53.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.227.164.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.195.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.147.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.212.109.229	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.179.116.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.91.215.6	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-28-2016-08:04:00 to 02-28-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	192
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	117
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.76.127.44	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
212.76.127.111	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
2.52.128.30	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
107.167.105.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.32.179.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.5.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.219.193.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.60	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
40.77.167.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
121.28.150.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
109.253.158.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.21.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.140.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.226.60.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
121.28.150.154	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.83.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.4.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.158.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.41.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.187.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.124	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
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.189.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.48	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.93.252	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
2.54.48.236	Israel	147.237.77.216	dover.idf.il	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	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
209.88.198.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.210.206.180	France	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
213.57.244.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.120.145.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

02-28-2016-08:04:00 to 02-28-2016-09:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.169.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
109.253.146.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
37.26.148.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
176.13.4.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
80.246.137.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
85.65.151.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	8
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/resources/styles/	Block	4
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
79.182.135.132	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	3
176.13.3.145	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	3
69.197.169.202	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 69.197.169.202	Block	3
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.137.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.36.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.20.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.5.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.205	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	3
46.19.85.32	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
31.168.21.80	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.52.11.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.133	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
2.52.157.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.158.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
109.253.195.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
213.57.244.119	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.228.187.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.22.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl07.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
69.197.169.202	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/1298.pdf	Block	1
131.253.25.140	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.172.170.93	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.76.106.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.76.106.127	Block	1
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.253.214.169	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	1
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
213.168.248.212	Ireland	147.237.77.216	dover.idf.il	Unknown HTTP Request Method PURGE in URL www.idf.il/english/	Block	1
84.228.230.41	Bulgaria	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
192.118.48.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
66.249.66.179	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
80.246.133.152	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
212.76.106.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
121.28.150.154	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/^http:/	Block	1
217.132.26.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
69.197.169.202	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-23134-he/shared/usercontrols/headerupper/	Block	1
66.249.69.33	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/110005.pdf	Block	1
149.86.187.92	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

02-28-2016-08:04:00 to 02-28-2016-09:04:00