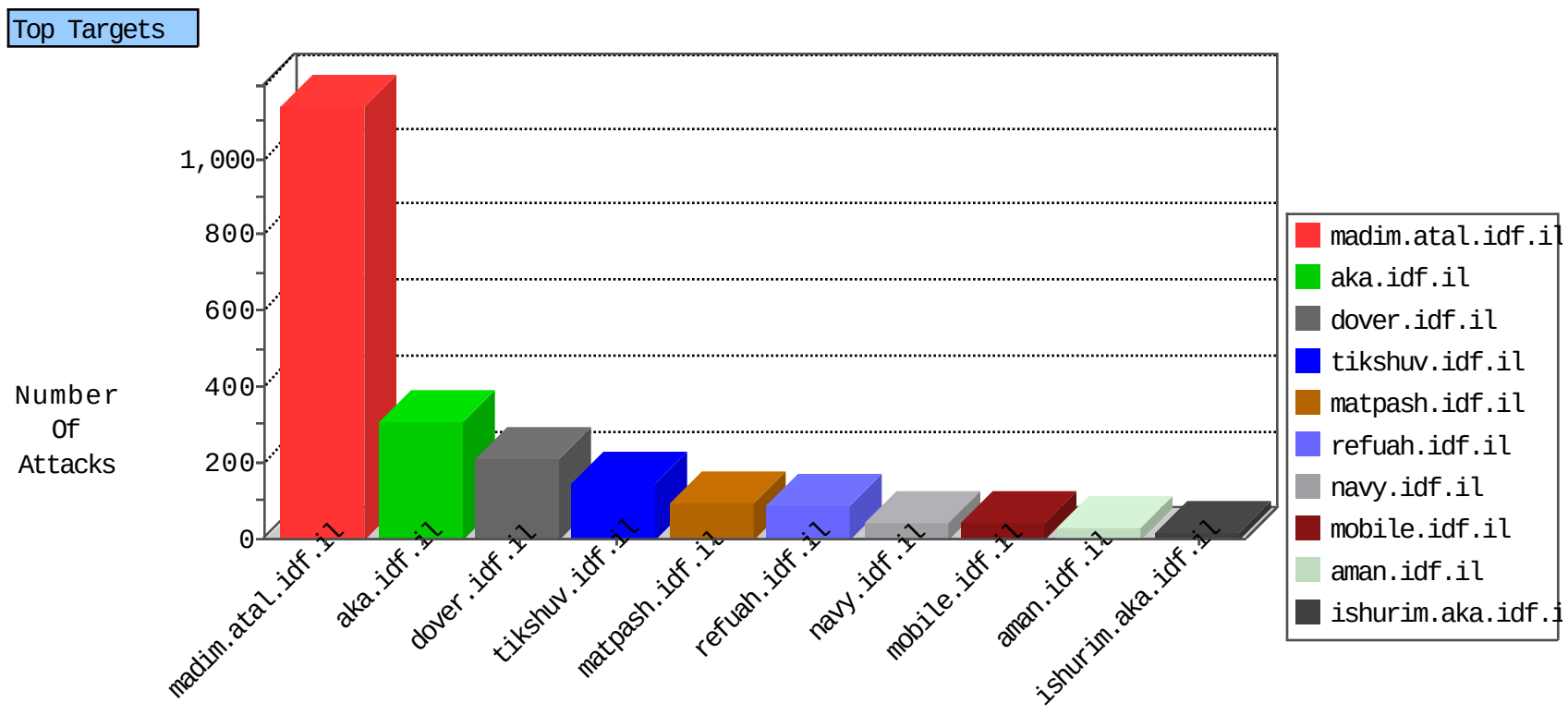
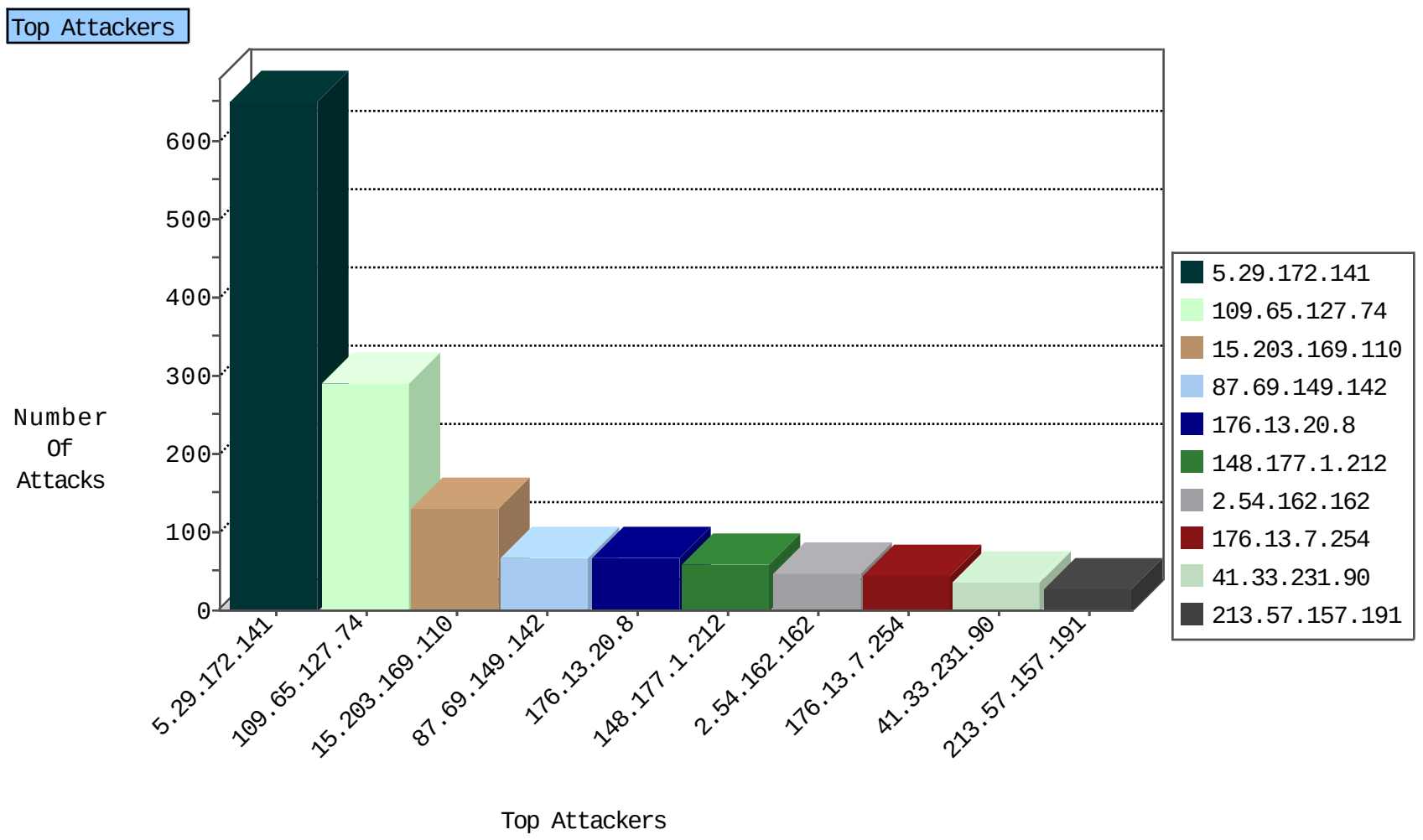
02-16-2016-20:04:00 to 02-16-2016-21:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-16-2016-20:04:00 to 02-16-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	49
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.201		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.78	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-20:04:00 to 02-16-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.63.188.181	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.185.43.135	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
172.86.83.125		147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1

02-16-2016-20:04:00 to 02-16-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
93.63.188.181	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.64.171.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
2.54.49.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
152.97.21.204	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
111.207.243.73	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
109.186.49.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
84.110.7.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
79.182.145.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
157.55.39.72	147.237.0.34	United States	tikshuv.idf.il	SERVER-IIS asp-dot attempt	1
149.78.96.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.129.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.230.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.103.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.9.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.77.176		matpash.idf.il	ET SCAN Potential SSH Scan	1
79.181.213.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.179	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1

02-16-2016-20:04:00 to 02-16-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
15.203.169.110	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	130
87.69.149.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
148.177.1.212	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.157.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
149.78.215.21	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
213.57.157.191	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.54.162.162	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.142.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
109.253.141.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
95.35.158.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
77.75.92.142	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.146.155	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.24.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.101.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.253.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.149.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.155	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.253.145.127	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.142.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.88	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.253.7	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.158.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.120.73.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.117.142.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.117.142.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.194.198.213	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.242.130	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.52.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.188.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.128.141	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.5.20	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.3.144.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.117	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.145.127	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.75.92.252	Lebanon	147.237.77.216	dover.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
46.19.85.117	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.52.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.179.172.128	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.198	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.182.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-20:04:00 to 02-16-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	338
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	290
109.65.127.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
109.65.127.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.20.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
109.65.127.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	46
176.13.7.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.162.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
5.29.172.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	24
109.253.134.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
79.183.36.180	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.183.36.180	Block	9
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.209	Block	8
149.88.105.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.88.105.72	Block	6
79.183.36.180	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
79.178.3.33	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.3.33	Block	4
176.13.13.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.13.13.20	Block	4
88.240.145.96	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 88.240.145.96	Block	4
149.88.105.72	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
213.8.204.34	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8516-he/himush.aspx#.vsnan78l1bo.facebook	Block	3
77.127.208.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.208.77	Block	3
217.132.45.57	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 217.132.45.57	Block	3
172.86.83.125		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 172.86.83.125	Block	3
79.182.48.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.48.79	Block	3
109.65.117.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.208.77	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
37.142.159.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
88.240.145.96	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
94.65.158.9	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
217.132.45.57	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	2
88.240.145.96	Turkey	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 88.240.145.96	Block	2
79.182.48.79	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.233.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.55.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
92.98.126.75	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/slider.js	Block	1
172.86.83.125		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cgi-bin/php	Block	1
87.69.224.138	Israel	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
37.59.29.19	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/.	Block	1
148.251.21.227	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.182.48.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
213.8.204.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
5.28.186.167	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 5.28.186.167	Block	1
2.52.128.141	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
88.240.145.96	Turkey	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.3.147.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-16-2016-20:04:00 to 02-16-2016-21:04:00