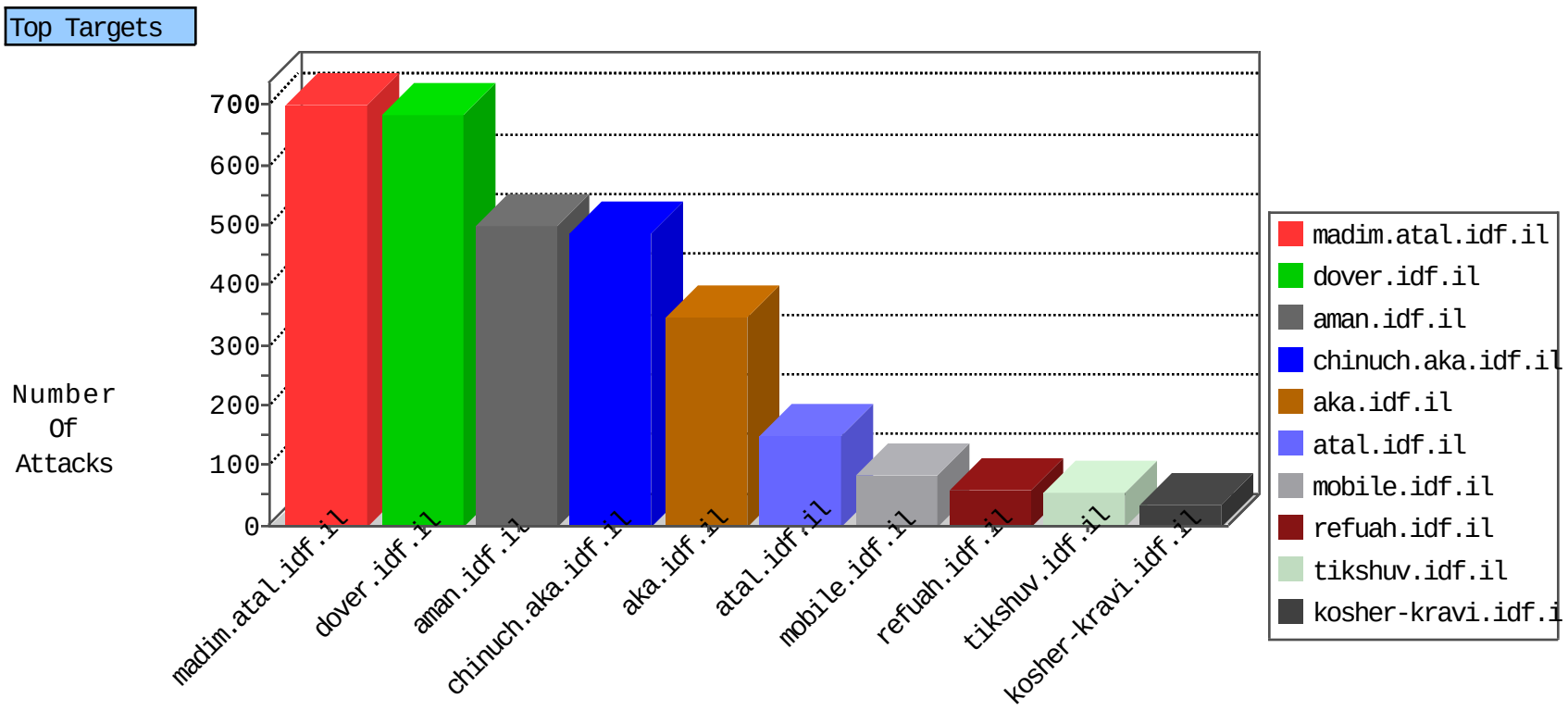
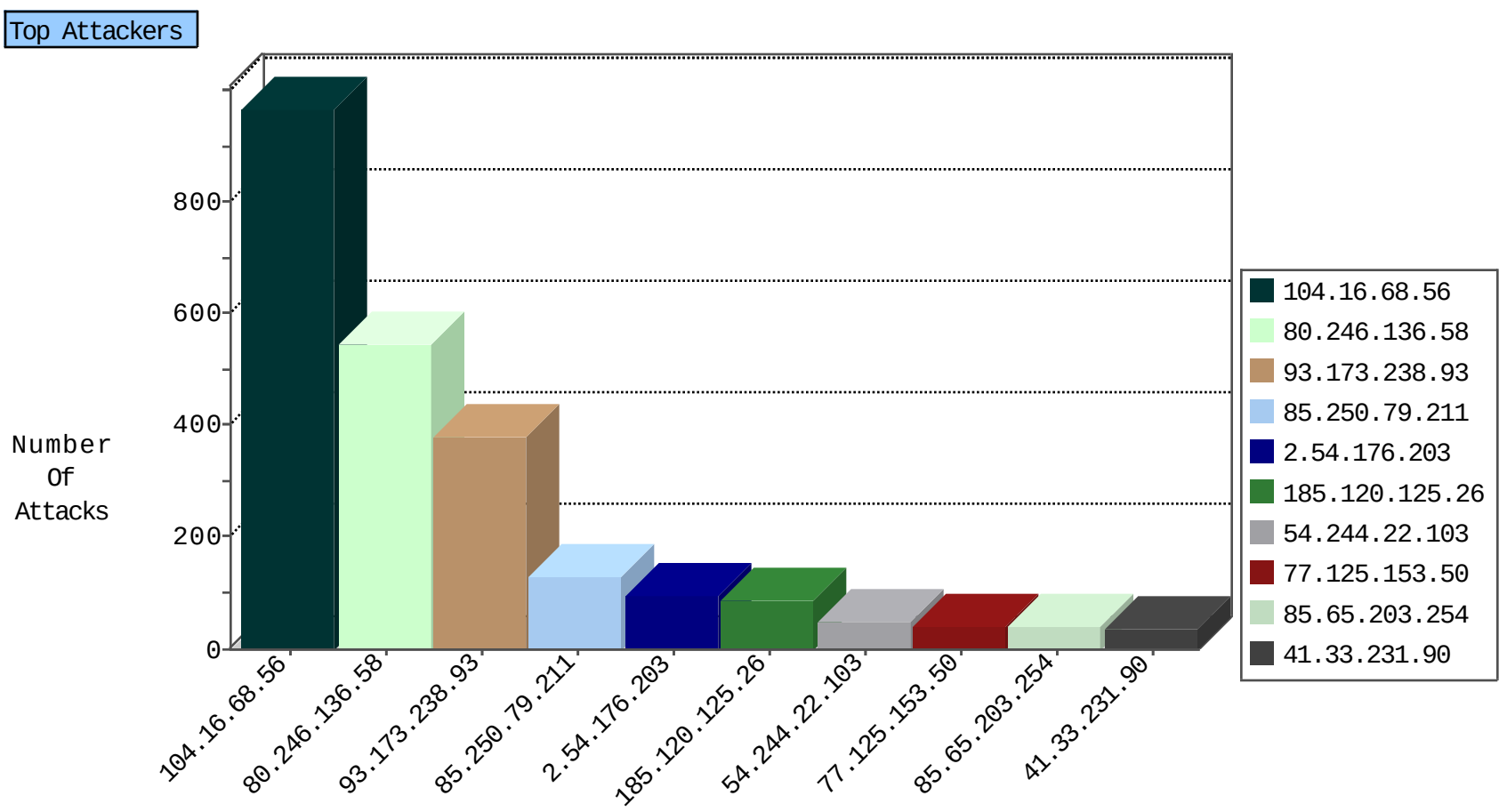
02-07-2016-21:04:09 to 02-07-2016-22:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-07-2016-21:04:09 to 02-07-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
172.98.84.44		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	39
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
31.202.128.149	Ukraine	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
77.125.79.114	Israel	147.237.72.167	ishurim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-07-2016-21:04:09 to 02-07-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.98.3.81	Netherlands	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-07-2016-21:04:09 to 02-07-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.58	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
121.141.225.10	147.237.76.147	Korea, Republic of	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.56.93.171	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.207.60.30	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.109.234.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.65.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
176.228.26.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
175.99.87.209	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
121.141.225.10	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.56.93.171	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
121.141.225.10	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.110.110.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
175.99.87.209	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
175.99.87.209	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

02-07-2016-21:04:09 to 02-07-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.68.56	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	484
104.16.68.56	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	483
85.250.79.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	116
93.173.238.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
77.125.153.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
185.130.5.207		147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	30
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.173.147.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
85.65.203.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
85.130.137.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.250.79.211	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
212.179.219.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.179.219.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.65.203.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.54.130.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.215.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
31.210.187.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.127	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
45.63.97.227		147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
212.179.219.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.20.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.168.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.240.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.203.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.151.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.65.203.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.201.5.200	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
85.65.203.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.9.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.189.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
128.138.65.203	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.189.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.189.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.229.40.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.189.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.209.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.54.189.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.32.179.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.173.147.84	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
141.0.15.214	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.244	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-07-2016-21:04:09 to 02-07-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.238.93	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.173.238.93	Block	315
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.58	Block	128
2.54.176.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.58	Block	42
176.13.0.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
87.68.78.151	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
2.54.176.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
2.54.137.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.54.128.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.146.219	Block	11
89.139.156.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.88.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.9.177	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1777	Block	3
93.173.147.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.120.191.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.248.31	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.108.248.31	Block	2
37.26.146.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
2.54.18.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.59.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.59.60	Block	2
213.57.136.149	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
109.253.209.227	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.125.153.50	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
37.26.146.201	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.240.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.64.59.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
85.250.79.211	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $41 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.136.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
5.29.155.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $103 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
118.193.222.243	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
77.126.20.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
62.151.24.138	Spain	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.108.248.31	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
2.54.141.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion $1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.9.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.170	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.64.151.28	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 109.64.151.28	Block	1
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $87 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.154.156.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
213.151.38.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18328-he/dover.aspx&sa=u&ved=0ahukewiyyom7sebkahvlvxqkhq-1dzcqfggjmak&usg=afqjcngvpkktdqxhwzzaew18tttnckud_a	Block	1
83.130.100.170	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
141.212.122.81	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /x	Block	1
77.127.158.42	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
62.151.24.138	Spain	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
95.86.88.91	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1

02-07-2016-21:04:09 to 02-07-2016-22:04:09