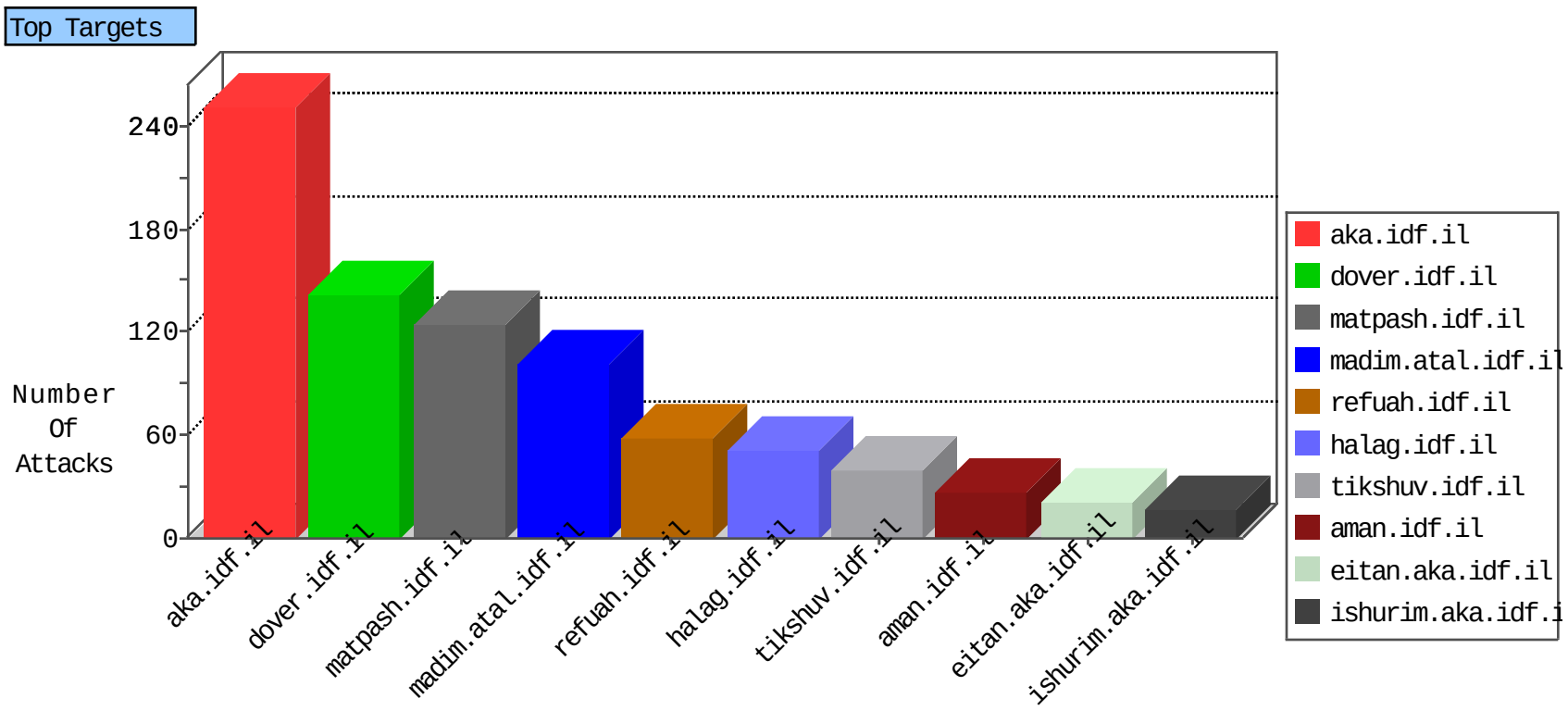
02-16-2016-14:04:08 to 02-16-2016-15:04:08

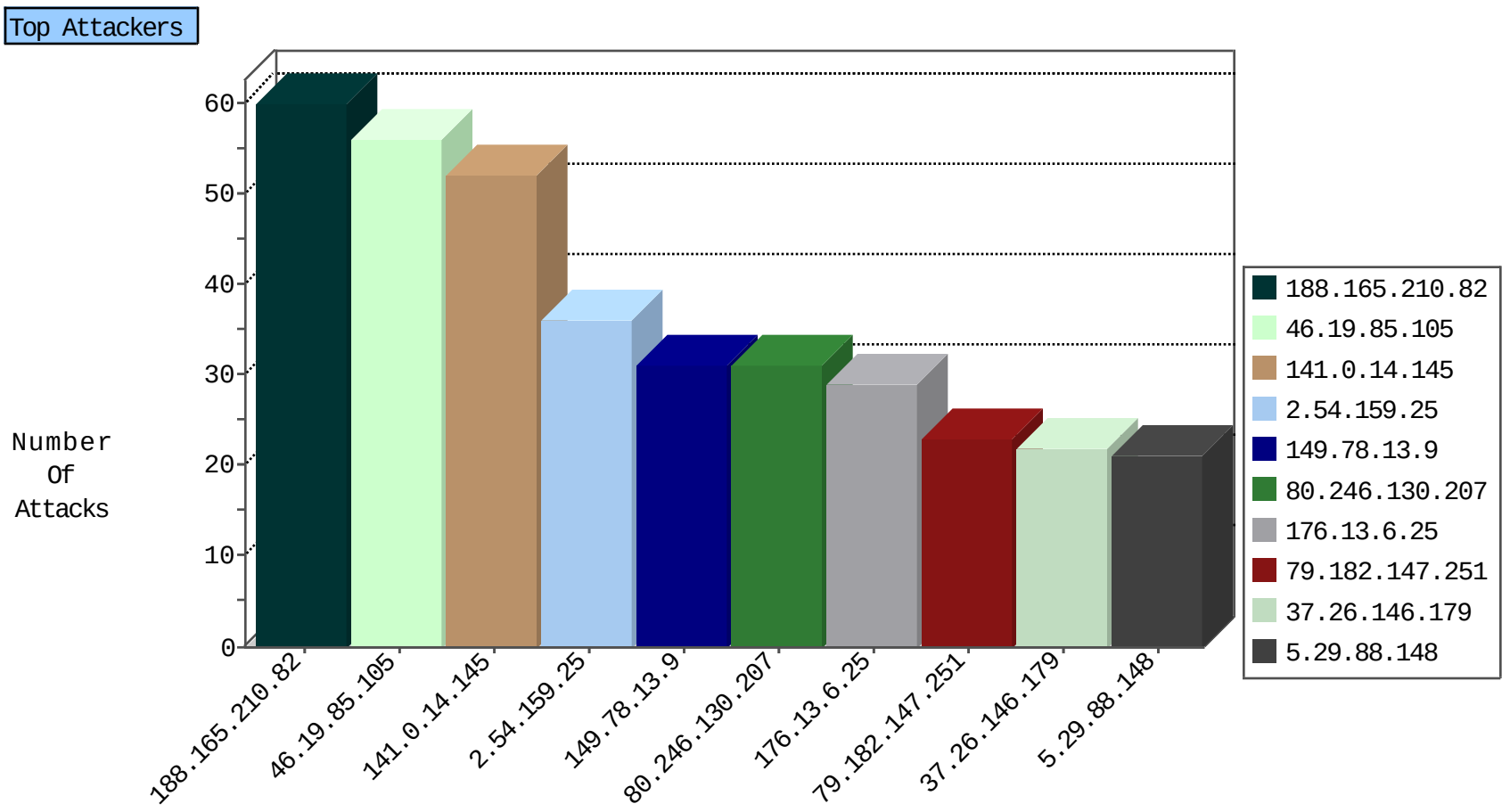
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
173.208.206.205	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
78.189.223.136	Turkey	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.210.82	France	147.237.77.176	matpash.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	4
92.29.219.30	United Kingdom	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
122.164.95.45	India	147.237.77.74	law.idf.il	14062: HTTP: SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)	Block	1
188.165.15.162	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.165.210.82	147.237.77.176	France	matpash.idf.il	Tehila - Perl LWP with fake user agent	6
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
109.253.145.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.130.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.44.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.73.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.172.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.178.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.201.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.137.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.24.204.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.179.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.21.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.60.210.31	147.237.77.216	Singapore	dover.idf.il	portscan: TCP Distributed Portscan	1
89.243.214.238	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.172.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.49.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.208.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.165.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.145	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	52
2.54.159.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.78.13.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
80.246.130.207	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
37.26.146.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.147.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	17
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.13.1.121	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.108.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.156.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.62	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.147.251	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.1.121	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.70.18	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.41	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.5	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.41	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
94.230.86.24	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.23.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.115.83.5	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.6.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.195.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.223.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.183.195.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.223.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.10.177	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.145.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.113.125.11	Romania	147.237.76.39	mobile.meitav.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
79.179.196.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.128.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.188.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.180.113.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.21.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.133.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.64.208.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.176.162.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.239.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-14:04:08 to 02-16-2016-15:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
176.13.6.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
188.165.210.82	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	21
188.165.210.82	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.165.210.82	Block	21
5.29.88.148	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
188.165.210.82	France	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 188.165.210.82	Block	6
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.71.31.161	Block	4
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
217.132.152.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.127.112	Block	3
176.13.16.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.178.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	3
109.253.198.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.159.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.161.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.161.178	Block	3
2.54.132.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.161.178	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.253.206.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.215.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.121.119.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.95.126	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/authenticationservice.asmx	Block	2
79.182.168.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
37.26.148.133	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.66.223.173	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
91.73.108.225	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
217.194.198.104	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method Â?sX[[#28]]oÂŒÂ§Ã£Ã§Â°8 in URL Ö·×€Öµ^xz×³..3[[#5]]â€¹&Â°Âš×?,yd~8Â³Â§mÂ¸ ×Ÿ Â¶4Â®3Â?[[#28]]â,¬×'Â²×³[[#20]]n[[#21]]	Block	1
41.79.66.144	Nigeria	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL ;nÂ·Âž[[#19]][[#11]]w%8Âš [[#16]]:;~_dÂ¶[[#18]]d5Â?h×°Âµ[[#1]]×–wlÖ¿[[#19]]×¨neÖ¿	Block	1
84.94.82.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.235.103.203	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
141.212.122.193	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.115.83.5	Block	1
176.13.15.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$98 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
95.86.103.37	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1279-he/cogat.aspx&sa=u&ved=0ahukewjs-63rovzkahwcd5okhr11cpmqfggimaa&usg=afqjcneun8bgj6tyzckq_loom0posduz2a	Block	1
217.132.152.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$85 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.183.98.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.25.112.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.149.134	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Abnormally Long Request method	Block	1
2.54.143.115	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 2.54.143.115	Block	1

02-16-2016-14:04:08 to 02-16-2016-15:04:08