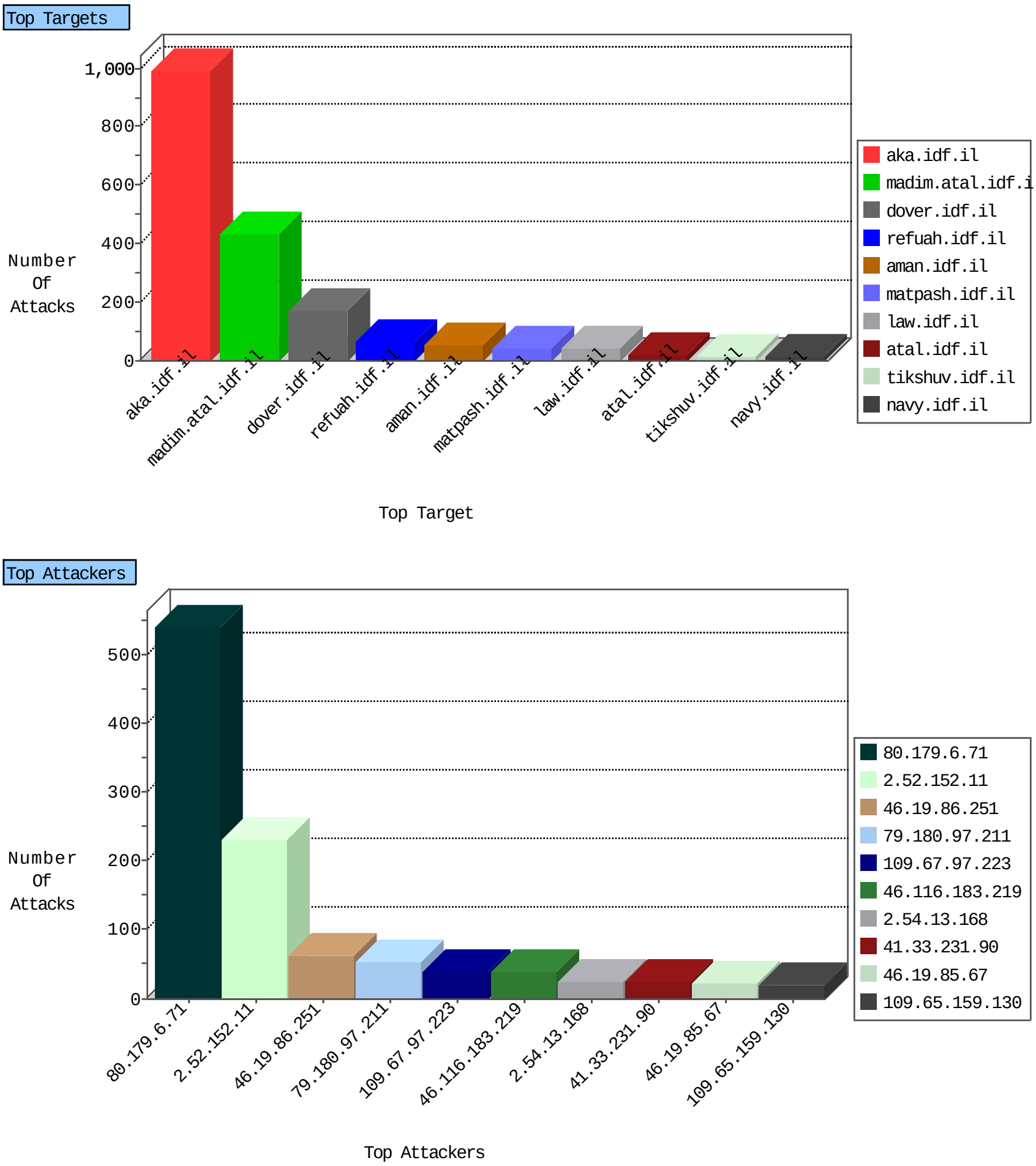
02-03-2016-16:04:07 to 02-03-2016-17:04:07

IDF Under Attack
Daily Report



02-03-2016-16:04:07 to 02-03-2016-17:04:07

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	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.67.140.231	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
188.138.1.218	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-16:04:07 to 02-03-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.249.142.199	China	147.237.77.216	dover.idf.i	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1

02-03-2016-16:04:07 to 02-03-2016-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
217.132.44.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
128.30.52.96	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.95.53.219	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.0.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.96.47.10	147.237.8.46	Kuwait	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.227.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.67.84.244	147.237.77.212	Taiwan	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.57.50.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.147.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.159.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.219.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.22.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

02-03-2016-16:04:07 to 02-03-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.6.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	540
109.67.97.223	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	24
109.65.159.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
95.35.167.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
84.108.183.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
71.172.52.7	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
2.54.13.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
37.26.148.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.77.3.200	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
94.230.86.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
199.203.151.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.34.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.50.29	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
130.193.50.7	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
31.176.246.22	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.67	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.147.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.139.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.120.148.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.139.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.29.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.2.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.67	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
147.236.138.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.47.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.130.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.60.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.74.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.24.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
93.158.152.46	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
212.29.225.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.22.130.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.101.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.15.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.186.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.242.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.161.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.195.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-16:04:07 to 02-03-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.152.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.52.152.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
79.180.97.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.52.152.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.152.11	Block	19
84.108.212.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
2.54.48.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.20.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
176.13.14.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.52.2.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.137.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
219.94.163.62	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.163.62	Block	5
109.253.142.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.104.128.158	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 46.116.183.219	Block	2
2.54.186.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.13.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$87 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 46.116.183.219	Block	2
87.69.66.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$56 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 46.116.183.219	Block	2
85.65.199.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$90 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
183.89.25.72	Thailand	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/5/1705.jpgï»¿	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 46.116.183.219	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 46.116.183.219	Block	2
79.179.24.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 46.116.183.219	Block	2
109.253.144.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$81 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 46.116.183.219	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 46.116.183.219	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 46.116.183.219	Block	2
131.253.25.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.116.183.219	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 46.116.183.219	Block	2
110.249.142.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/login.action	Block	1
5.28.184.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.117.17.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.32.179.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#23]][[#3]][[#3]][[#0]](Ã¨ in URL	Block	1
79.180.97.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.177.173.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.186.184.144	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.116.183.219	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at Â¢Â€Â¿Â©ÃŠ ÂµÂ¸ÂµÃ±[[#11]]Ã¬Ã®Â²Ã‘Â¾Ã°Ã›RYÃ™mÂšÃ¶[[#21]]ÂµÃ‘Ã¹Ã“ s^Ã¤Â¨ÂƒÃ°[[#8]]Ã¾Â¸[[#7]]RÃ˜Â 3[[#24]][[#4]]D&Â½Â´MqÂªÂ†ÃŽ [[#29]]LXÃ€Ã¯Ã #[[#20]]Â«ÃªÃŠÃ‡Â¶Ã·ÃƒÃšÃ¨Ã^Â±8wÂ¦Â^ [[#2]]Ã?Â‹Â·Ã^~Â–$O8^Ã¼Â¦Â¨Ã«Ã˜;Ã œ[[#12]]YÂ, Ã-Ã µ[[#23]]Â QÃ»TÃ?Â°Â¥vÃ”fÂ»[[#26]]Ã»10[[#0]]Â?Â€4xÃ«[[#3]]Wi g[[#1]]!QN[[#8]][[#0]]Bw<[[#16]]Âš/Â‘Â§GÂ?Â·Â‡Ã¦8Â–•32Ã°'Ã€ >Ã¬[[#0]]ÃŸÂ‘Ã“Ã³ÃŒÃ„Â-=6Ã‘Ã?+[[#19]]tÂµÃ?~Â“dÃ¦Ã¾Â, [[#27]][[#27]]Ã–&Â¹ÂŒQ•#Â½ÃŽ\e8Ã•[[#25]]Ã…Â½GÃ?Â–Â— Â³nÂ»Â«b[[#21]]Ã’XÂ–[[#4]]Ã„Â”^FÂ©ÃŒH	Block	1
85.64.72.32	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-03-2016-16:04:07 to 02-03-2016-17:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
83.166.234.5	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1

02-03-2016-16:04:07 to 02-03-2016-17:04:07