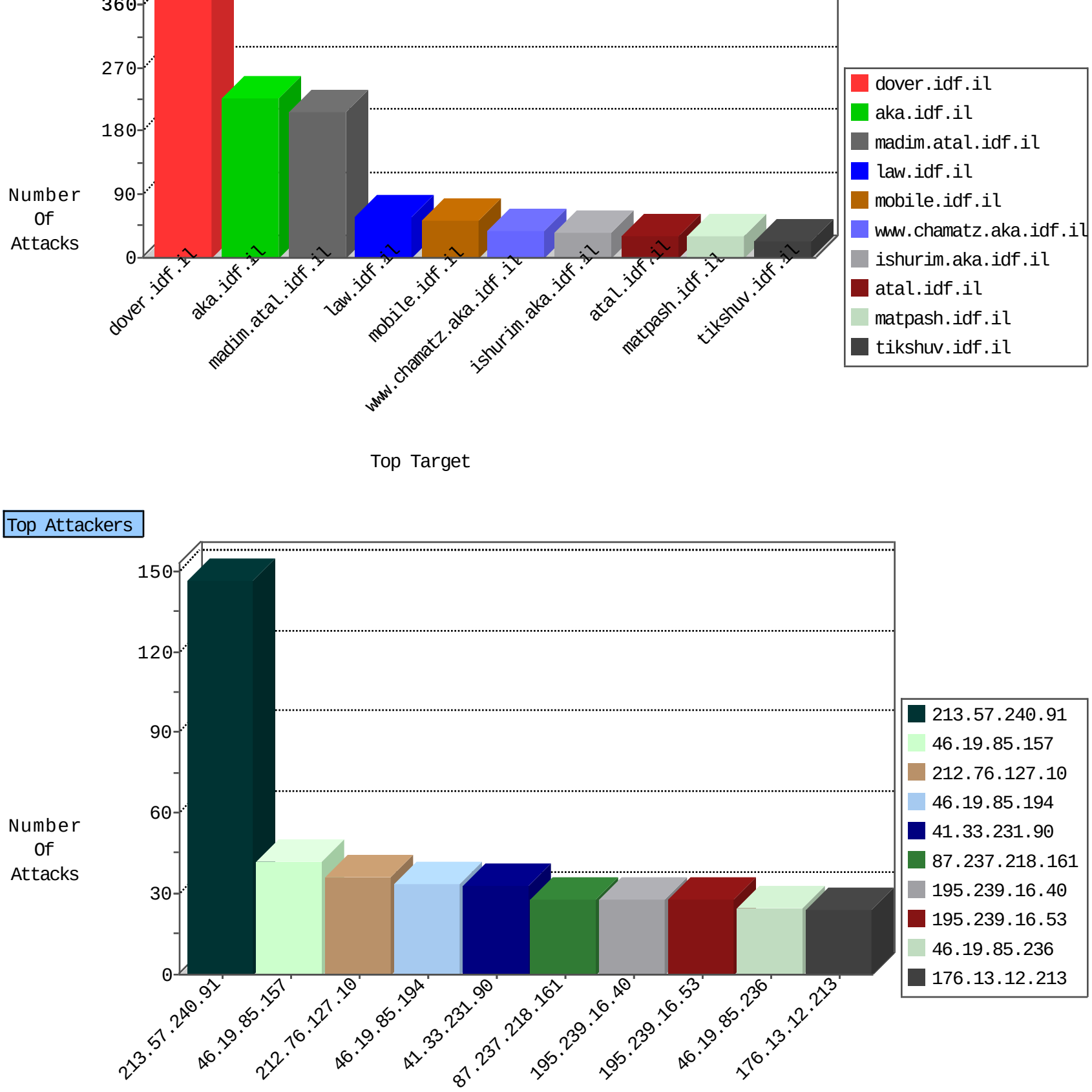
02-03-2016-23:04:04 to 02-04-2016-00:04:04

IDF Under Attack
Daily Report



02-03-2016-23:04:04 to 02-04-2016-00:04:04

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
51.254.23.234	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
78.186.113.19	Turkey	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.212	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
51.254.23.234	United Kingdom	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-23:04:04 to 02-04-2016-00:04:04

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	2

02-03-2016-23:04:04 to 02-04-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.75.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.148.22.26	147.237.77.216	Lithuania	dover.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.77.178	Lithuania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
217.132.152.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.76.147	Lithuania	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
175.6.228.149	147.237.76.34	China	yohalan.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
46.148.22.26	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
95.224.38.18	147.237.76.34	Italy	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
46.148.22.26	147.237.72.166	Lithuania	aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.81.218	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.8.28	Lithuania	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.235	China	sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
37.200.225.36	147.237.0.15	Oman	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.93.106.48	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.148.22.26	147.237.77.212	Lithuania	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.199	Lithuania	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.38	Lithuania	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
94.44.182.159	147.237.76.31	Hungary	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.148.22.26	147.237.72.156	Lithuania	aman.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
37.200.225.36	147.237.0.19	Oman	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1

02-03-2016-23:04:04 to 02-04-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
87.237.218.161	Germany	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
37.26.146.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
79.177.205.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
89.138.222.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.144.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.127.157.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.178.227.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.108.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
185.3.144.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
92.241.56.25	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
5.102.254.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.121.97.21	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.156.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.147.239	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.54.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.185.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.19.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.63.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.232.87	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.218.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
89.138.218.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.64.93.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.69.69	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4

02-03-2016-23:04:04 to 02-04-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.13.12.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
109.253.218.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	8
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	8
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	8
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 213.57.240.91	Block	8
2.54.144.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 213.57.240.91	Block	5
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.240.91	Block	5
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 213.57.240.91	Block	4
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 213.57.240.91	Block	3
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	3
89.138.222.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
76.115.96.90	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 213.57.240.91	Block	3
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 213.57.240.91	Block	3
176.13.3.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.62.239	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.178.111.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.68.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.65.104.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Query String from 213.57.240.91	Block	2
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.207.164	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.29.93.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.211.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 213.57.240.91 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
46.19.85.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
149.88.234.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 213.57.240.91	Block	2
5.102.212.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$45 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.15.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$60 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.246.136.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.117.46.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.64.192.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	NULL Character in Method Ã™OÂ·Â„Ã¯Â´<Ã›[[#11]]Ãª 3[[#3]][[#21]]Ã¤Â‡Â Ã¡[[#7]]EÂ¨lÂ‹u*Ã¨bÂ±Â°Â½Â¤Ã²Â¥Â¶Â©Â” mwÂ®[[#27]]JqÂ»1Ã¼[[#5]]Ã„Â•Ã°&Q8Â›L#[[#26]]gÂˆi"o[[#0]]Â®w@Ã¤Ã, `DÃ«Â´ÂˆÂ°Ã²r&	Block	1
213.8.204.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.23	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
89.138.72.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 213.57.240.91	Block	1
185.35.62.11	Switzerland	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
50.22.11.11	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
5.28.175.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$22 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.110.210.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-03-2016-23:04:04 to 02-04-2016-00:04:04