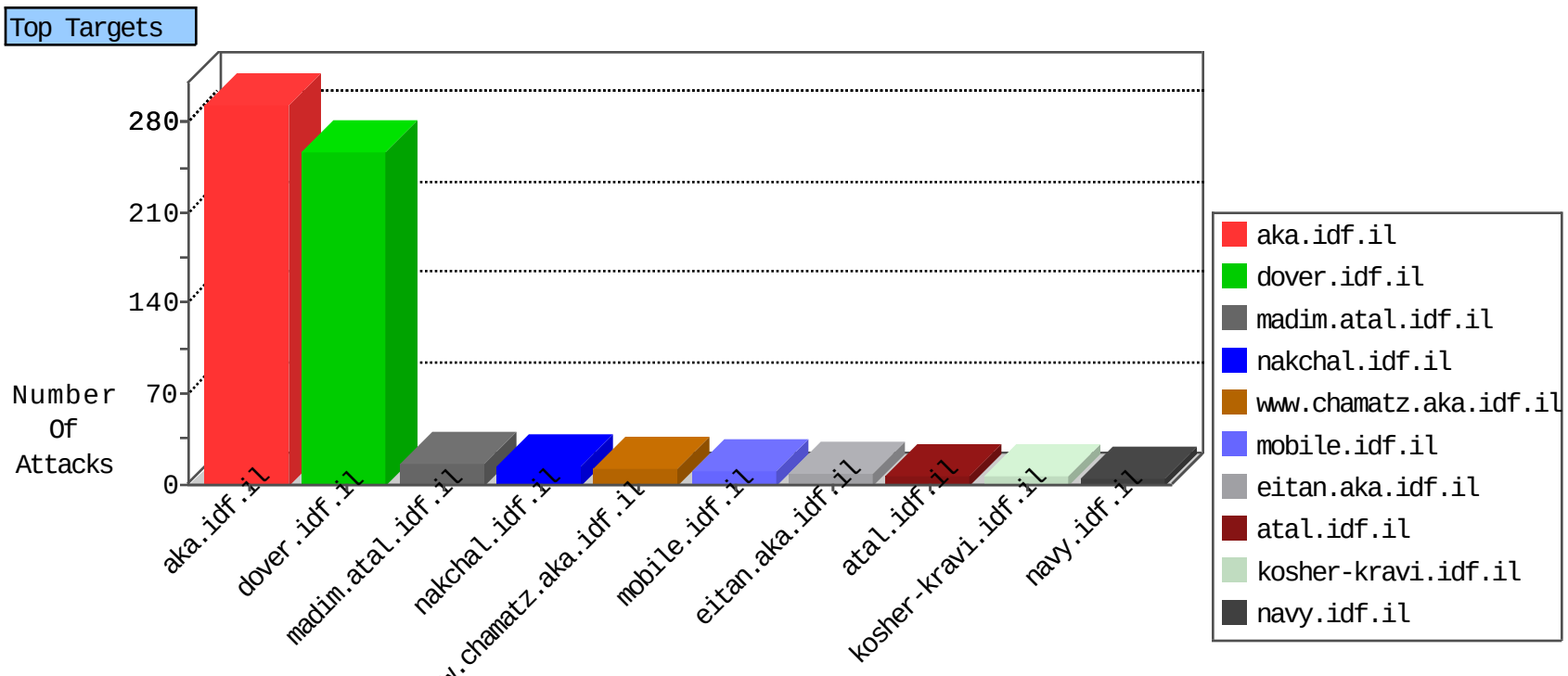
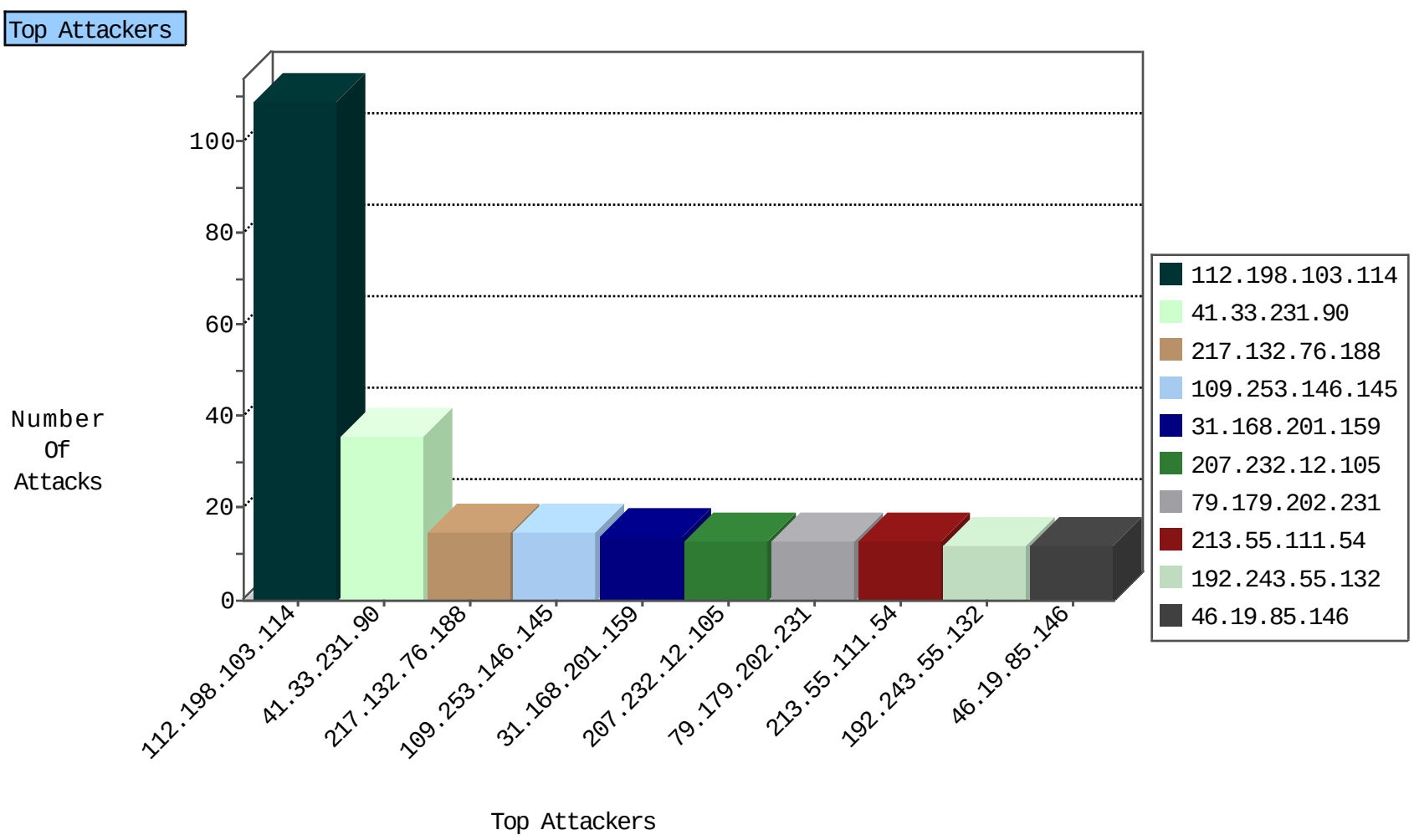
02-04-2016-06:04:01 to 02-04-2016-07:04:01

IDF Under Attack Daily Report





02-04-2016-06:04:01 to 02-04-2016-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
14.162.147.234	Vietnam	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.77.226	www.chamatz.aka.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
74.91.28.61	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1

02-04-2016-06:04:01 to 02-04-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-04-2016-06:04:01 to 02-04-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.197.208.36	147.237.0.35	Slovakia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.197.208.36	147.237.0.15	Slovakia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.123	147.237.8.46	Moldova, Republic of	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.197.208.36	147.237.0.33	Slovakia	idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

02-04-2016-06:04:01 to 02-04-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
31.168.201.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.76.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.55.111.54	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
76.18.176.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.146.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
50.159.130.59	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.7.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.179.202.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.232.12.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.91.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.68.148.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.146	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
70.195.200.38	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.147.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.232.12.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.146.145	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.76.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.10.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.114	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
68.180.228.25	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.182.160.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.147.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
68.180.228.25	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
64.233.172.177	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.162.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.215.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.148.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.124.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.199.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.181.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.33.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.97.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
157.55.39.173	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-04-2016-06:04:01 to 02-04-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.130.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.103.114	Block	3
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 112.198.103.114	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.103.114	Block	3
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
185.32.179.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.103.114	Block	2
192.243.55.132	Dominica	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/headerupper	Block	1
89.139.142.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.137	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 10	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
109.66.116.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.163.3	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
201.92.33.236	Brazil	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 201.92.33.236	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
89.248.174.4	Netherlands	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
185.32.179.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Malformed URL [[#16]]×™×”Â©#Â?Â¿â‚ª$×©	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteytkufa	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/chinuch/gallery	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Too Many Headers per Request - 68 Headers	Block	1
79.179.202.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$11 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.62	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
201.92.33.236	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/terrestres	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¸Â?Ã£'[[#20]]tK[oBÂ´[[#23]]Âª¥Â¿Ã¦Ã¥:Â¼I<Ã œ -/H$Ãª_[[#14]]!Ã«_FqmÂ™Âºv)[[#17]] Â‹Ã-Âˆ+Â»Â´Ã˜	Block	1
192.243.55.132	Dominica	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
89.248.174.4	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 112.198.103.114	Block	1
73.211.169.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
79.179.202.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â¸Â?Ã£'[[#20]]tK[oBÂ´[[#23]]Âª¥Â¿Ã¦Ã¥:Â¼I<Ã œ -/H$Ãª_[[#14]]!Ã«_FqmÂ™Âºv)[[#17]] Â‹Ã-Âˆ+Â»Â´Ã˜ in URL [[#16]]×™×”Â©#Â?Â¿â‚ª$×©	Block	1
66.249.69.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 1 for [[#16]]×™×” Â©#Â?Â¿â‚ª$×©	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59334&docid=68033	Block	1

02-04-2016-06:04:01 to 02-04-2016-07:04:01