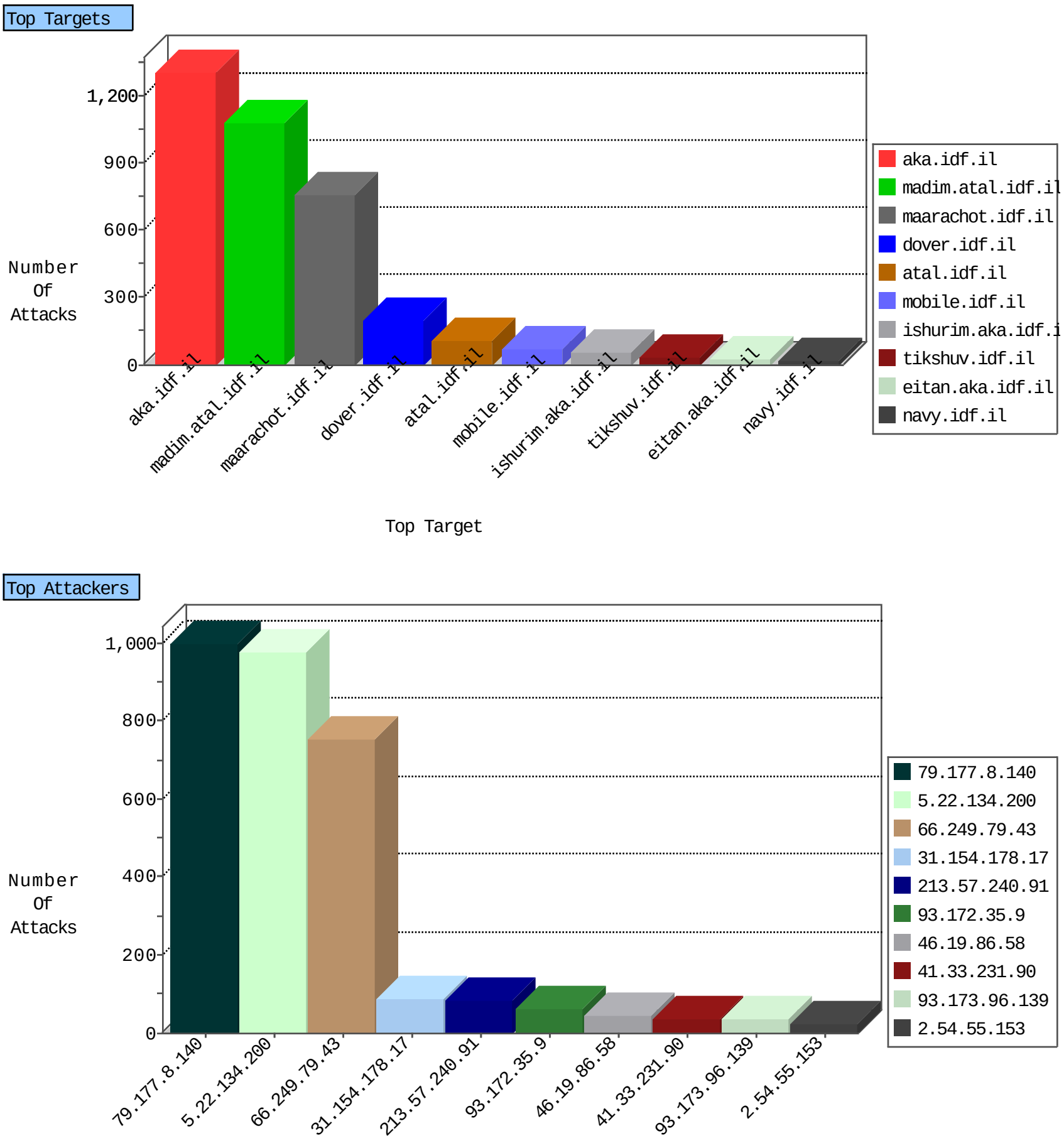
02-05-2016-13:04:06 to 02-05-2016-14:04:06

IDF Under Attack
Daily Report



02-05-2016-13:04:06 to 02-05-2016-14:04:06

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	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
104.207.128.23	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-05-2016-13:04:06 to 02-05-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.79.193.230		147.237.77.216	dover.idf.il	C104: HTTP: Access to - pageinfo.php	Block	1
188.165.15.206	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-05-2016-13:04:06 to 02-05-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	754
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.106.92.137	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
41.228.12.4	147.237.72.166	Tunisia	aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1

02-05-2016-13:04:06 to 02-05-2016-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
93.172.35.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
46.19.86.58	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.19.86.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
84.228.56.252	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
2.54.152.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
207.241.231.229	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	10
2.54.38.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.3.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
157.55.39.248	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
5.102.254.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.228.34.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
196.217.42.135	Morocco	147.237.77.216	dover.idf.il	drop		drop	6
79.176.107.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.6	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.230.86.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.74.127.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.9.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.158.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.168.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.8.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.138.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
197.42.188.164	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.210.187.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.108.99.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.16.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.16.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.138.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.49.229	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.54.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.53.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1000
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.134.200	Block	527
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 5.22.134.200	Block	345
5.22.134.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
93.173.96.139	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
2.54.55.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.32.179.83	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	Multiple Illegal Byte Code Character in Method from 213.57.240.91	Block	8
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 213.57.240.91	Block	6
85.65.49.94	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.49.94	Block	6
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method 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 Header Name from 213.57.240.91	Block	5
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 213.57.240.91	Block	5
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.228.34.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.102.54.114	Algeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.74.127.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
41.102.54.114	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	3
31.154.253.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.130.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 213.57.240.91 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	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
79.179.38.169	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$45 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 213.57.240.91	Block	2
107.182.20.202	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
40.77.167.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	NULL Character in Query String 4×ª× V×?[[#26]]×,[[#0]]Â-×ƒ[[#24]]$â€ž:[[#1]]Â¬Ã–ÃŸ[[#16]][[#8]][[#0]][[#28]]Ö¶U× Â»2?×¥Â¡2oÃ»pÂ°×¥lâ€™8wRÂš?Ã·Ã¿KwgÃ? on 9[[#28]]^ÂŸË†â„¢×¥mÖµÂŽÂŠÖ¶	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
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	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL txuÂ¦[[#6]])Æ'[[#27]]Â¾[[#22]]m[[#24]][[#23]][[#16]]Ã›y×?gÖ¶dâ€?×¤×£:c[[#1]]×,×œÖ²[â,¬â,ª"×'[[#19]]×´â€™ÂŸmjj~7Ã?`1/Ãœ	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ~[[#31]]Ö¸nmÖ½×©Â¯×€×ƒ[[#23]]vâ€¹[[#25]]Ö²â,¬Â?48[[#31]]aÖ³Ö½n\Â?Â³[[#19]]iÂšy×?ÂœÂ²×¢â€"^×?ÃšÂ?Â¶×›Â¬Â¡q6Â¸×¡Ö¾×šwaÂ?3Â¼~â€œâ€?Ö°m[[#28]]iÖ¾(Ã›â,ª×?ev3xÂ²tÂ²y[[#23]]Â²3â€˜}â€˜[[#19]]ÃŸâ€˜8Â¢Â¡[[#23]]Â 1eÂ½Ã¿â€?x<l×›[[#1]]~â€¦â,ªjÂ»â„¢[Ö¹â€?Â³t[[#30]][[#3]]Ö³6-6â€œ<×§ayÃžÂ¢×?â€š[[#21]]`[[#4]]Â´Â?×ŸË†×³[[#15]]×?×±Ö³â€žâ,ª×Ÿ[[#24]]×š;Â-r{ertqÃ›ÂŸ%%â€ž$	Block	1
213.57.240.91	Israel	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
79.183.28.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$102 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Malformed URL	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request method	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding)![Fi}(&X-FO_PdXK/L0-[xhX1YtKq1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
107.182.20.202	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
40.77.167.70	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name 9Â¸•ÃœpÃ·yÃŠÂ¬Ã¾Â´Ã§Ã®[[#4]]ÂžÃ'7Â'QÃ¬Ã«[[#16]]`Â›qdÂ¡Â…Ã£[[#5]]^wÂ·	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.228.34.19	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
213.57.240.91	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method GÃºÃ¨Ã Â›Ã›)Â?KUÂ‡•&`Ã?@Ã•2b3Â–Ã¿*QÃ"!\jÃ™<[[#27]]ÃšxÃ†Ã±Ã°V%Ã´Â…[[#17]] in URL	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
77.127.157.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$113 in aka.idf.il/main/giyus/questionnaire.aspx	None	1