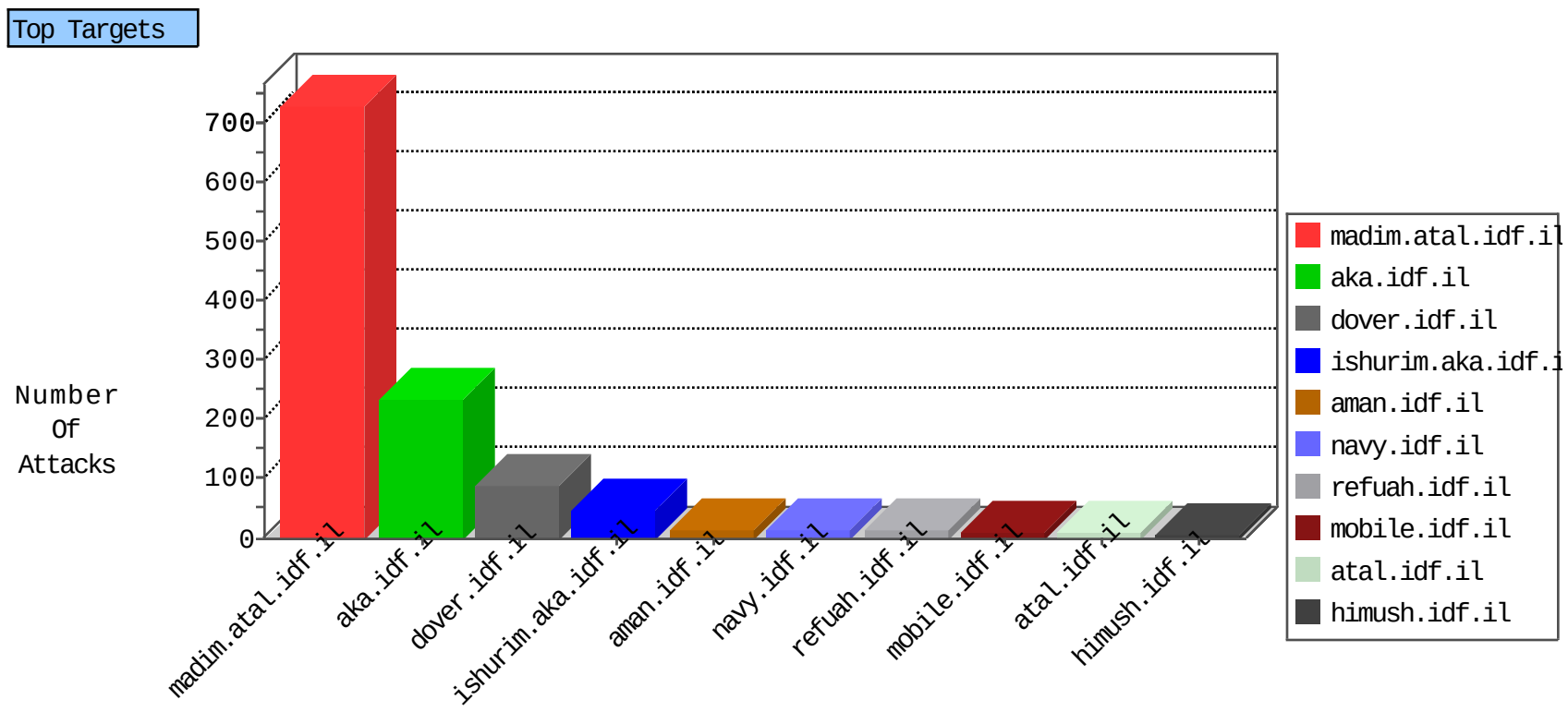
02-10-2016-07:04:05 to 02-10-2016-08:04:05

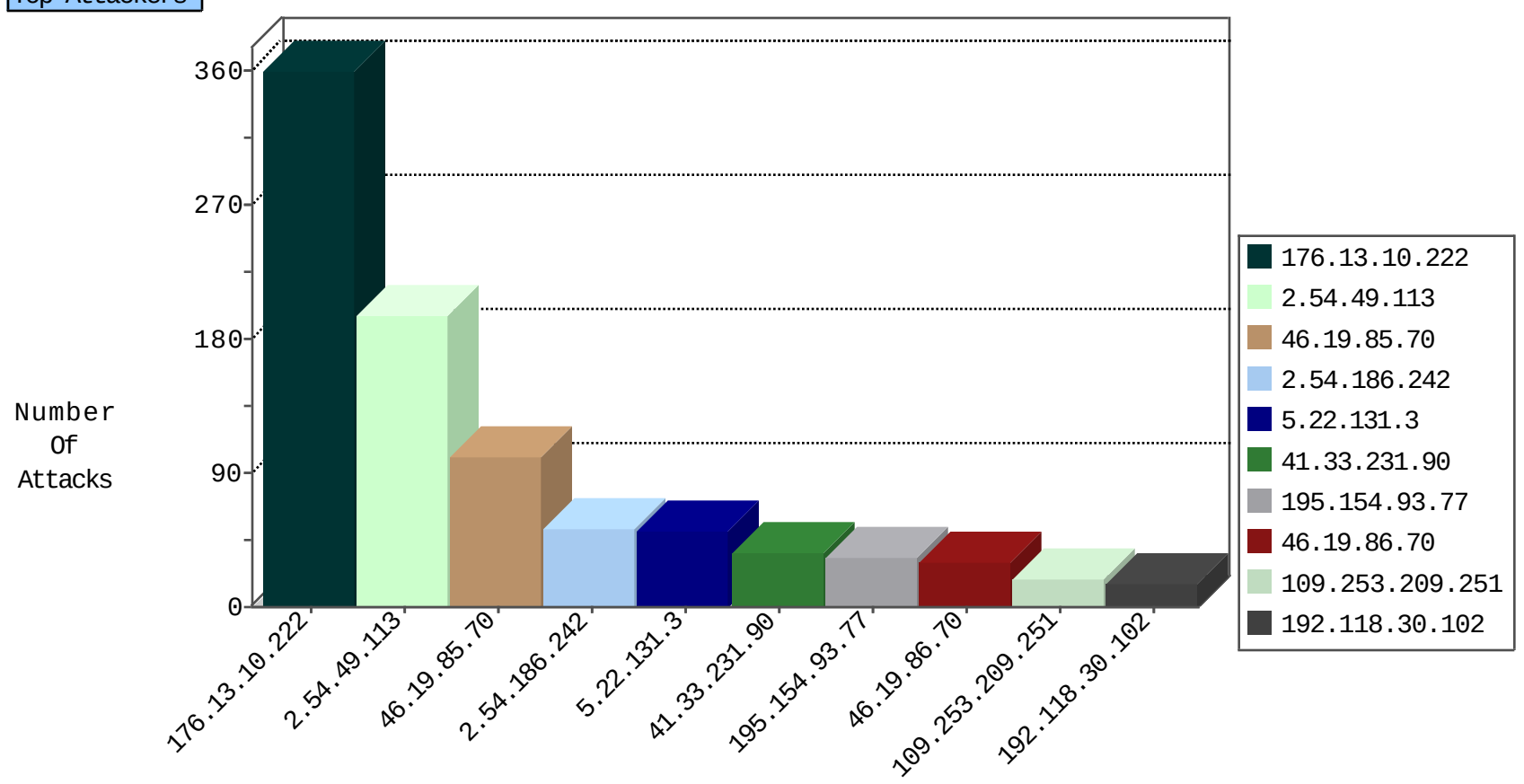
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-10-2016-07:04:05 to 02-10-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
45.63.8.39		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

02-10-2016-07:04:05 to 02-10-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
206.180.246.167	Canada	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-10-2016-07:04:05 to 02-10-2016-08:04:05

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
66.249.65.238	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.249	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
85.93.5.64	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
78.92.76.221	147.237.8.14	Hungary	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
185.3.147.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.67	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1

02-10-2016-07:04:05 to 02-10-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.70	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
2.54.186.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
109.253.209.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
81.218.198.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.186.242	Israel	147.237.72.166	aka.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
2.54.186.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.186.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.186.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.187.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.186.187.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.186.242	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.159.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
184.63.76.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.202.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.199.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.78.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.136.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.64.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.154.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.139.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.159.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.213.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.32.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.154.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.197.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.125.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.50.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.161.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-07:04:05 to 02-10-2016-08:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
176.13.2.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.5.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.179.9.115	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.177.174.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

02-10-2016-07:04:05 to 02-10-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.10.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	174
2.54.49.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
176.13.10.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
176.13.10.222	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.10.222	Block	70
2.54.49.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
5.22.131.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
80.246.136.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.157.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.70	Block	3
2.54.49.113	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
2.54.24.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
2.54.186.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 195.154.93.77	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 195.154.93.77	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 195.154.93.77	Block	2
109.67.170.241	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 195.154.93.77	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 195.154.93.77	Block	2
2.54.44.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Malformed URL from 195.154.93.77	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 195.154.93.77	Block	2
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 195.154.93.77	Block	2
2.52.38.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.1.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.176.154.204	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 10 for)t_râ€œdupd[[#19]]Â¡×¦Â¿=fÂ®.uÃ·â€œÂŽÃ¿Ã™[×˜â€“0sÃ¿×›	Block	1
176.48.183.59	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Malformed URL)t_râ€œdupd[[#19]]Â¡×¦Â¿=fÂ®.uÃ·â€œÂŽÃ¿Ã™[×˜â€“0sÃ¿×›	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
5.39.222.159	Netherlands	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/rom-0	Block	1
2.52.62.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Too Many Headers per Request - 39 Headers	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL)t_râ€œdupd[[#19]]Â¡×¦Â¿=fÂ®.uÃ·â€œÂŽÃ¿Ã™[×˜â€“0sÃ¿×›	Block	1
185.32.179.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 195.154.93.77 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Ã‹6Âƒ[[#24]][[#24]]8ÂµQÂ› •[[#19]]Â–Ã¨[[#18]]Ã¯Âš[[#31]] Â¼Ã¡yjÃ·Â¾Â¬Â?%D!Ã?Â?Â¡ÂŒÃ¬=(Â±}Â·Â„`cZÂº)ÂŸ^D^[[#26]]Ã«Ã—83Â®Ã™Â?Â§ÃŸ9Ã§Â»\Ã••Ã¿XÃ‰[[#6]]ÃŽÃŸ[[#6]]fÃ°Ã¶Ã—@Â”Âƒ >,Ã¼Â?Â©Ã²YDÃºÃ»ÂªÃ°FÂ•[[#5]]Ã£Ã±[[#3]]rE,%!xÃ¡ÂµÃ¯ÂœÂ³Ã‰Ã’ [[#17]]GÃ£LÃ?Â,yÂ—Â¶;ÃžÂ¡*QÂ•ÂœEÂ-<Â¤V`q[[#23]]Ã, jPÃ°Â°Ã¹SÂ?[[#6]]IÂ—Ã†ÃŸ	Block	1
5.39.222.159	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/rom-0	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Unknown HTTP Request Method }[[#7]]Â‹!AÂ¸Ã?X:Â^*Â™bVÃµÃ, Â¿oÃ¹Ã¶[[#20]]KÃ“[[#24]]ÂŒv[[#26]]QÂŠ-Ãµ^]Â¬Ã¥w+Â¸Ã«aÂšÃžÂ [[#30]]!Ã¥Ã¿XS[[#28]]+Ã, Ã©Ã³s2Â¤75kÂ¢[[#26]]Â¦Ã½<[[#27]]Ã¹Â¨Â¡Â»Ã¹Ã£[[#24]]Ã¼(fEÃ¶p-[[#3]]Â‹[[#2]]K[[#29]]Ã?DD[[#11]][[#0]]yÂ¿Â¤.:s[[#23]]Â•Ã”[[#22]]`Ã‹ÂŒ1Ã—6e[[#4]]Â„[[#16]]Â³;T!Ã´Â‘D=Ã†,Â¥_Â¬ÃªÂ®Ã¥YÂ‹,JÃƒmkÃ—5p[[#15]]ÂŽ[[#5]][[#23]][[#14]][[#18]]Â„E^[;Ã¶[[#30]]Â½YIÃ»ÂžÃ°.Â¤ in URL)t_râ€œdupd[[#19]]Â¡×¦Â¿=fÂ®.uÃ·â€œÂŽÃ¿Ã™[×˜â€“0sÃ¿×›	Block	1
81.218.141.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 195.154.93.77	Block	1
46.120.106.173	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
195.154.93.77	France	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
185.32.179.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-10-2016-07:04:05 to 02-10-2016-08:04:05