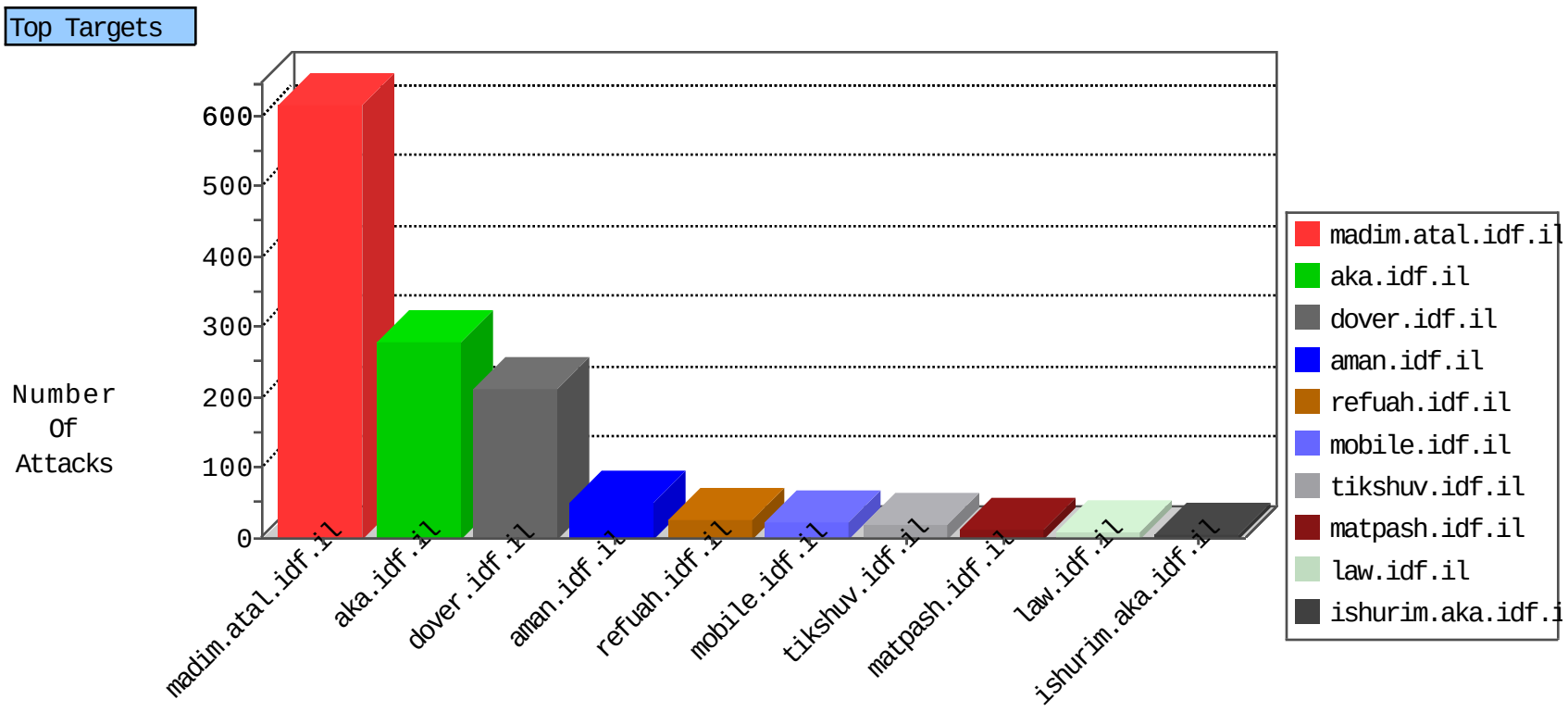
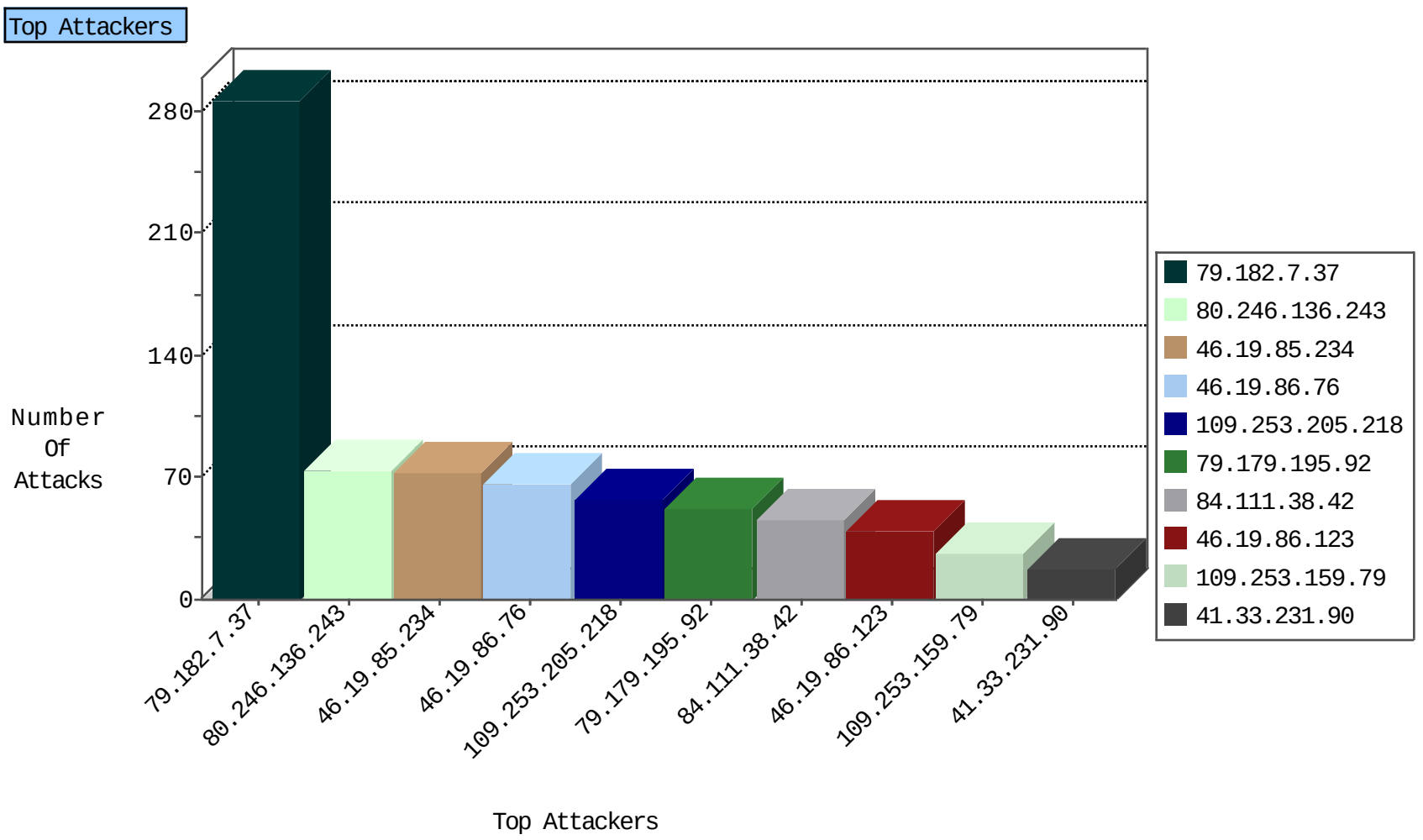
02-09-2016-11:04:02 to 02-09-2016-12:04:02

IDF Under Attack
Daily Report





02-09-2016-11:04:02 to 02-09-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.195.92	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	51
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
89.46.102.242	Romania	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.62	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-09-2016-11:04:02 to 02-09-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2

02-09-2016-11:04:02 to 02-09-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.183.7.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.154.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.216	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.153.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.95.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.80.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.56.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.195.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.89.119	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.73.198.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.58.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-09-2016-11:04:02 to 02-09-2016-12:04:02

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	18
2.52.56.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.177.63.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.116.218.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
77.127.55.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.168.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.135.11.15	Ukraine	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.169.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.155.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.188.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.102	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.26.180.188	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
217.194.202.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	4
46.19.85.23	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.15.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.114.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.241	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.27.105.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.60.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.134.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.206.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.127.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.131.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.173.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.220.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.236.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
176.13.8.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.33.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
62.0.209.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

02-09-2016-11:04:02 to 02-09-2016-12:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.80.177.189	Israel	147.237.72.166	aka.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
79.182.7.37	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.182.7.37	Block	163
79.182.7.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
109.253.205.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
109.253.159.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
212.235.62.94	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.235.62.94	Block	15
95.35.80.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
109.253.146.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
93.173.179.14	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 93.173.179.14	Block	5
79.182.7.37	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 79.182.7.37	Block	5
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.7.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.132.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 84.111.38.42	Block	2
14.200.79.77	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 84.111.38.42	Block	2
2.54.137.197	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
2.52.56.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	2
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 84.111.38.42	Block	2
2.54.168.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Malformed URL bf	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 84.111.38.42	Block	1
82.166.198.113	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name ÃˆÃŽ Â¯Â®_[[#7]]0Â¹'[[#31]][[#21]]•Â®2/GÃ–C[[#21]]XÃ‰![[#5]]6Ã¾6[[#7]]Â‹ [[#11]]'+6{Â§ÃšÃ-Ã¹[[#24]][[#26]]#Â›SÂ€Â™ÃŽÂ¥Ã¨Â“Â—4Â©Ã?Â±WÂ† Ã„X[[#16]]Â Ã–Ã,Ã´Â§[[#30]]Â¥Ã¯j[[#19]][[#17]]Ã?Ã-bÃ¹Ã…Ã?Â€I@N/Â“ rLÂ¬Bm5o'A2[[#5]]>3tÂ¶Â¼,DÃœlMÃ©ÂƒÂ´ÂŠÂ?ykÃ‰~Ã˜5;[[#31]]Ã˜ XU[[#14]]Â„''[[#0]]*;Ã«tÃµÃ–Â‰Âˆ sCÂ-Ã‘dÃ¸ Âª[[#25]], [[#29]] Ã³ÃŽ Ã°Ã?Â?([[#12]]Ã°Ã¸ Â²Ã¬ÂœÂ†ÃŠÃŸ[[#14]]Ã£IÂ‡Â€ W[[#7]][[#18]]*[[#11]]Â?Ã‘Â BNÂ‡qÃ»Ã¦WÃ¤DÂ›Â®Â?Â„ [[#16]]>[[#20]]8Ã£Ã„Ã´Ã?[[#24]]Â¹[[#15]]Â›~Ã˜Ã°Â²Â¸Â†Â	Block	1
79.179.54.231	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
188.6.142.140	Hungary	147.237.77.176	matpash.idf.il	Malformed URL towards	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at Ã“ 6Â¼[[#28]]Â˜Â·=Â¤ÃªÂ¸OÃ?oÃ† 05ÃµÂ?cgÂŽ[[#23]]Ã²Ã¶Ã‡sÃŸÂŽÂ‡ÃŠÂŽÃƒÂ¥Ãª?Â?Ã ÂŸ3Â€ 2Â°zÃº[[#23]]w$(Ã,Dr[[#16]]Â¯Â¬ÂšXÂ¯Â‹Ã…&Ã‰*Â†$P[[#20]]Â£NÃ½BÂ„ '[[#25]]Â„7Ã£Â›=Â«Ã±Ã?8Â¤*Ã,Â´Ãœ[[#8]]{Ã™Ã„Â†[[#6]]Â©[[#31]]Ã¼Â“ Ã¬Â³ÂµWpAOÂŒ#Ã'Ã¦Ã7Â½Â•Âº¤>)[[#27]]ÂŽÂ¯[[#15]]Ãƒ W[[#17]]fÂ»ÃœÃ©DÃ [[#15]]t!Ã±Âšo!Ã¦Â¤MÂ€0[[#12]]>Ã¯Â©Â³,Âž Ã£Â§LÂ¾X[[#26]][[#21]]Ã±Â,Ã½[[#29]]?Â€ [[#0]]A!vÃ?Â“ I1r[[#21]][[#22]]Âœw[[#15]]Â—EÃ¥2[[#17]]Ã Ã´[[#4]]Â–Ã‡SÂ°Ã´Ã› [[#5]][[#14]][[#22]]Ã¤&[[#22]]UÃ?G,[[#28]]Ã˜ÃŸÃ›D)	Block	1
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method [[#25]];Â™Â³[[#11]]Â†ÂŸÂµNÃˆyÂŽÂ“ Ã?PÃ”_Ã¥hÃ‰Ã?Ã¸ Âœl[[#1]][[#5]]Ã¬Ã«CÃ©EÂ'Ã€@ÃªÃ?Â‰tÂ¹$[[#31]]Â—9IÂ‰ZÂ©Ã'>ÃµÃ§=t,[[#6]]Ã [B([[#8]]Ã«Ã?-Â‹)ÃŠÃš4Ã§Â¿-Â§[[#18]]2ÃŸ 6Ã–Â€J!ÂºÂ»2Â—aÃ-Â€Ã³Â´[[#30]]Ã®E8QÃ›Ã£	Block	1
79.182.229.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 3	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
79.126.93.230	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
185.22.224.96	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
46.19.85.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 84.111.38.42	Block	1
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
84.111.38.42	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl107 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.235.62.94	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
84.111.38.42	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 84.111.38.42 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1