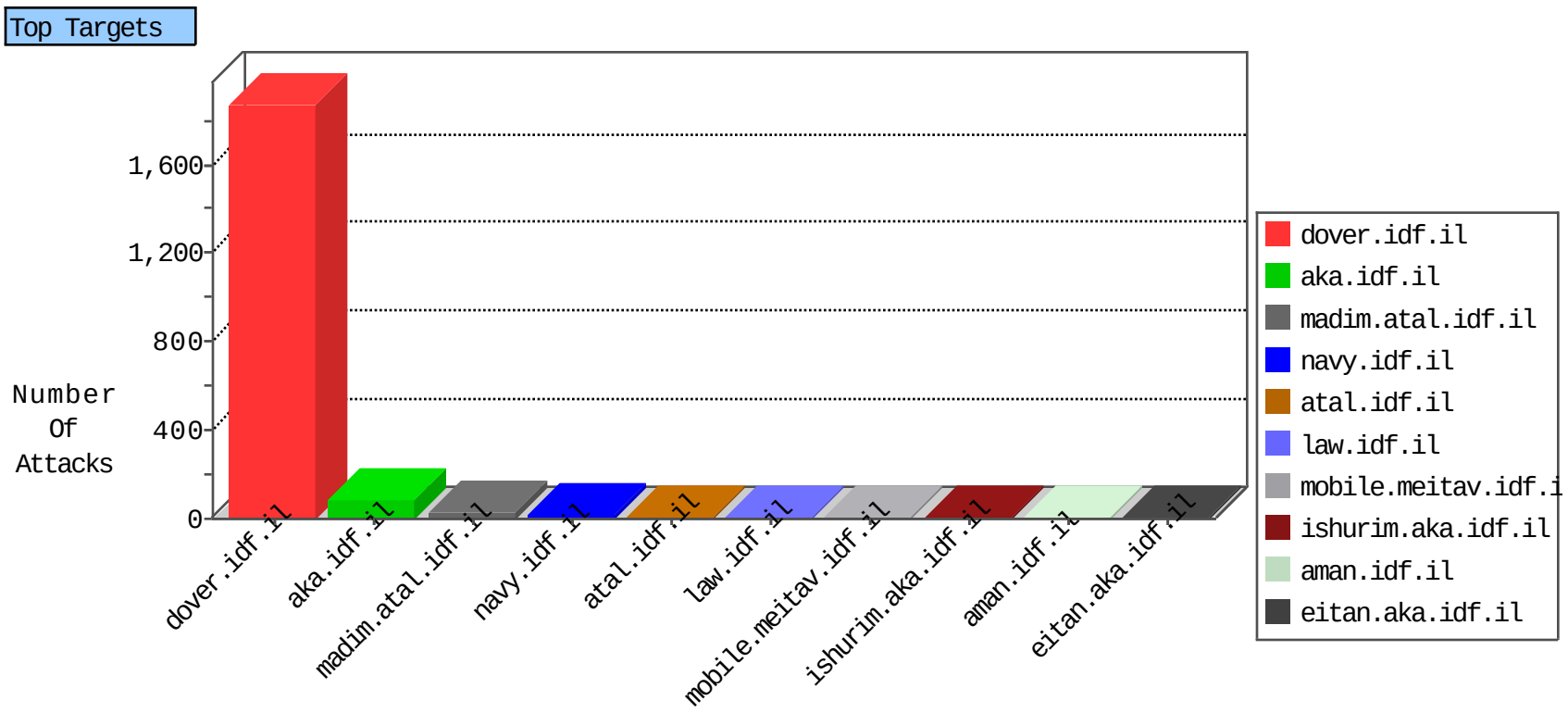
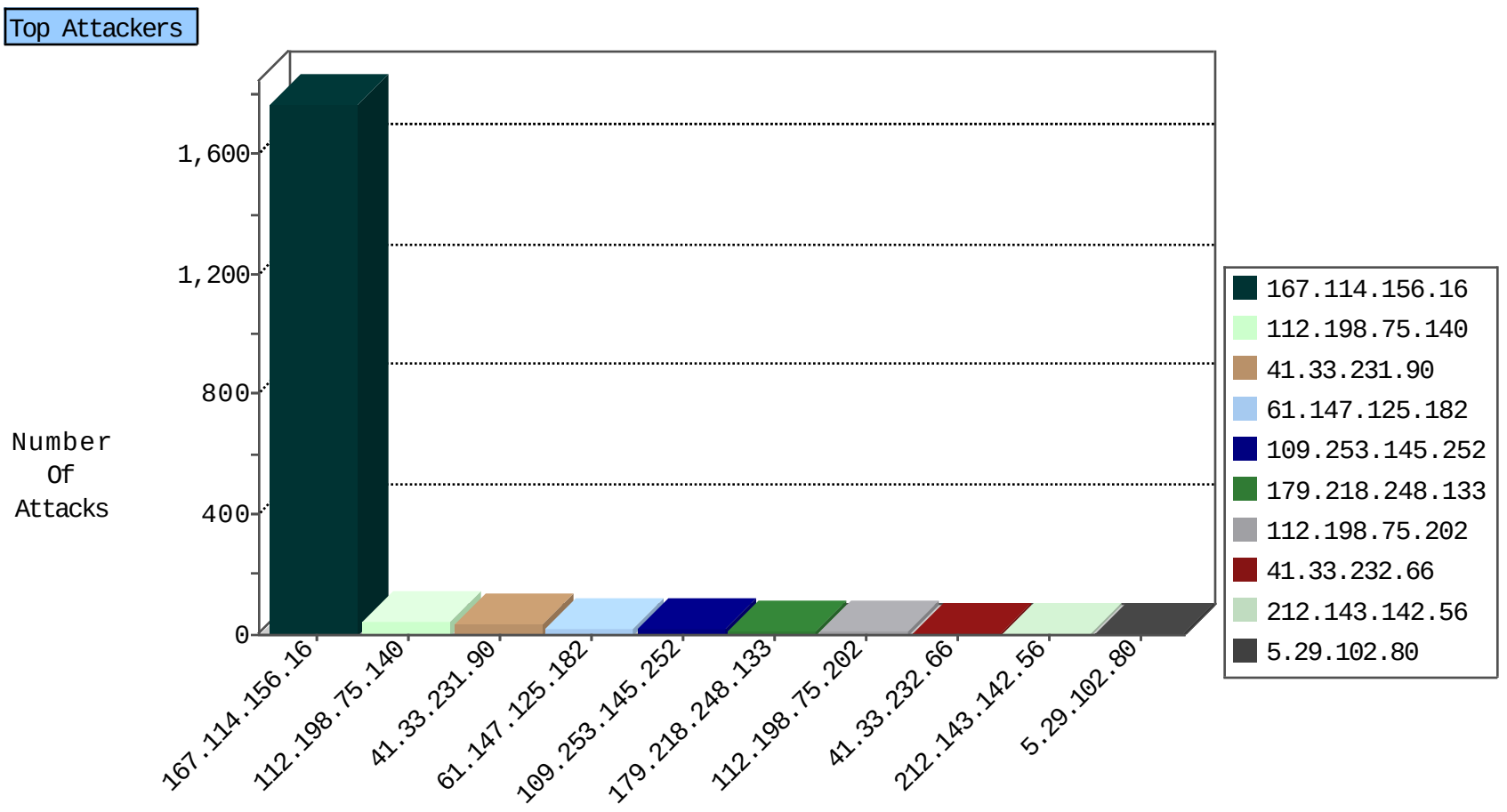
01-11-2016-06:04:08 to 01-11-2016-07:04:08

IDF Under Attack Daily Report





01-11-2016-06:04:08 to 01-11-2016-07:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3371
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	729
146.185.239.100	Russian Federation	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
23.95.248.111	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.111	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-06:04:08 to 01-11-2016-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	C076: HTTP: Access to - action=... (General)	Block	1

01-11-2016-06:04:08 to 01-11-2016-07:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

01-11-2016-06:04:08 to 01-11-2016-07:04:08

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
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
112.198.75.202	Philippines	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.30.24.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
179.218.248.133	Brazil	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.239	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
179.218.248.133	Brazil	147.237.76.86	navy.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
5.29.102.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
117.194.155.46	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.29.102.80	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
179.218.248.133	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.62.162.228	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
184.105.139.94	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.102.80	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.86.159	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.231	United States	147.237.0.33	idf.il	drop		drop	1
37.26.147.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
179.218.248.133	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
158.255.6.220	Russian Federation	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.84	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
76.107.33.15	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.95	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.62.2.87	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
46.19.86.159	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.14.236	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
158.255.6.220	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.90	United States	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
99.238.223.6	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.116	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.116.145.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.32.179.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.142.219.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.79	United States	147.237.0.35	akaws.idf.il	drop		drop	1
2.52.14.236	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
158.255.6.220	Russian Federation	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
109.65.148.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-11-2016-06:04:08 to 01-11-2016-07:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.145.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
61.147.125.182	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 61.147.125.182	Block	8
61.147.125.182	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 61.147.125.182	Block	8
109.253.139.48	Israel	147.237.0.19	madim.atal.idf.il	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
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	3
79.177.238.26	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
37.26.148.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.75.140	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.75.140	Block	2
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.75.140	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.75.140	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.75.140	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
61.147.125.182	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ewebeditor/admin/admin_login.asp	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name 1Â‡Ã¡~Â‘[[#3]]Ã¾Â‘;[[#3]]Â‡ Â¸Ã—Ã PKn&Ã?YÃœc]ÂŽÃ,[[#4]]Ã¶ÃƒQ]Â£)Â¸Â—Ã³[[#25]]g@Ã, Â¿[[#17]]Â•Â™5Ã¶nÃ¹pÃ¾0Â‰ÃŽÂ¤ÂÂ“Ã,[[#2]]ZÂ˜T4oÂŒ Ã?Â´Âª[[#12]]qtÂ’>Â?Â¸; Ãº;Â·/N'7L[[#20]]<ÃµÂ«K[[#23]]ZV[[#0]][[#25]]Ã¯Ã¯Â?ÃµÂ… By'M{[[#14]]Â‡Âˆ[[#8]]UÂ’]D[FlÂ¿ÂžnÂ>#!Â“Â¯,?Â¡ÃˆÂ±ÂŽ Ã½[[#21]]Ã©[[#1]][[#8]][[#3]]ÃŠ‰Ã—[[#5]]Â¯Â³	Block	1
77.125.5.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/giyua.aspx	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.75.140	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 18	Block	1
40.77.167.43	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sites/hoshen	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ÂŠ•Ã?BÂ«8Ã‹Â·Â¬Ã•Q#$r#ÂŒÃ¸ÂŽ Ã¼2Â‰Â©[[#6]]Â´[[#30]]Ã°Â‹Â”Ãž7MÂ¾+iÂ˜Ã?ZÂ¾pÂ¹Â´Ã¾{Â°_Ã… Ã?Ã…Ã‡[[#6]]Ã Â‹kÃ¨[[#15]]OÃ²Â»7cÃ“cEV>Â-D/Â-Ã› M^-Ã¨1Â¡[[#5]]Ã¸[[#24]][[#27]]nÃ”$Ã“ÃŒYÂ?[Â©Ã«Ã•_Â®Ã¬Â”Â²Âœ <Â‡[[#2]]Â?	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;w in www.aka.idf.il/main/giyus/captcha.ashx	None	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.75.140	Block	1
5.144.55.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.127.158.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/idfgdover.aspx	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Malformed URL	Block	1
61.147.125.182	China	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.139	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
31.168.226.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ÂŠ•Ã?BÂ«8Ã‹Â·Â¬Ã•Q#$r#ÂŒÃ¸ÂŽ Ã¼2Â‰Â©[[#6]]Â´[[#30]]Ã°Â‹Â”Ãž7MÂ¾+iÂ˜Ã?ZÂ¾pÂ¹Â´Ã¾{Â°_Ã… Ã?Ã…Ã‡[[#6]]Ã Â‹kÃ¨[[#15]]OÃ²Â»7cÃ“cEV>Â-D/Â-Ã› M^-Ã¨1Â¡[[#5]]Ã¸[[#24]][[#27]]nÃ”$Ã“ÃŒYÂ?[Â©Ã«Ã•_Â®Ã¬Â”Â²Âœ <Â‡[[#2]]Â?	Block	1
216.218.206.67	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	NULL Character in Header Name at R>[[#5]]Ã¦-CÂ¹y1[[#11]][[#2]]Â²Ãœ /Ã¤Ã´f27Ã²Â…mÃ?Ã˜Ã¬ÃˆÂ†@Ã€Â©Â·Â©Â›"Ã·GÂ’[Â”oÂ¬J	Block	1
66.249.66.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/894-he	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.75.140	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.66.25	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 112.198.75.140	Block	1
112.198.75.140	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL 1[[#28]]ÂŠ[[#3]]Â¢fhÂ¶c×˜ q/Â¬[[#21]]Â®q[[#27]][[#23]]b[[#12]]eÖ¿â,ªdÃ¿l[[#20]][[#20]]ÂŒ	Block	1
37.26.147.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-11-2016-06:04:08 to 01-11-2016-07:04:08