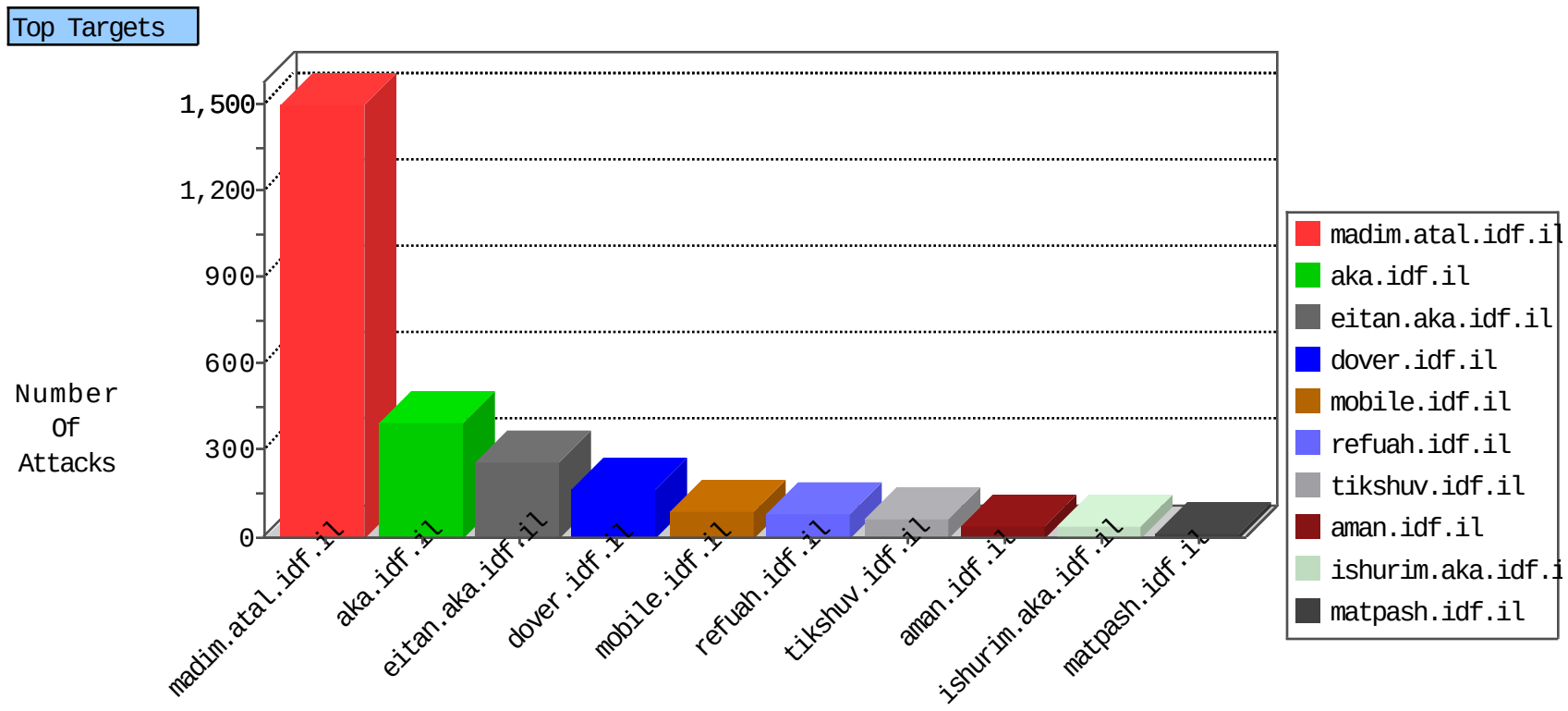
02-09-2016-14:04:00 to 02-09-2016-15:04:00

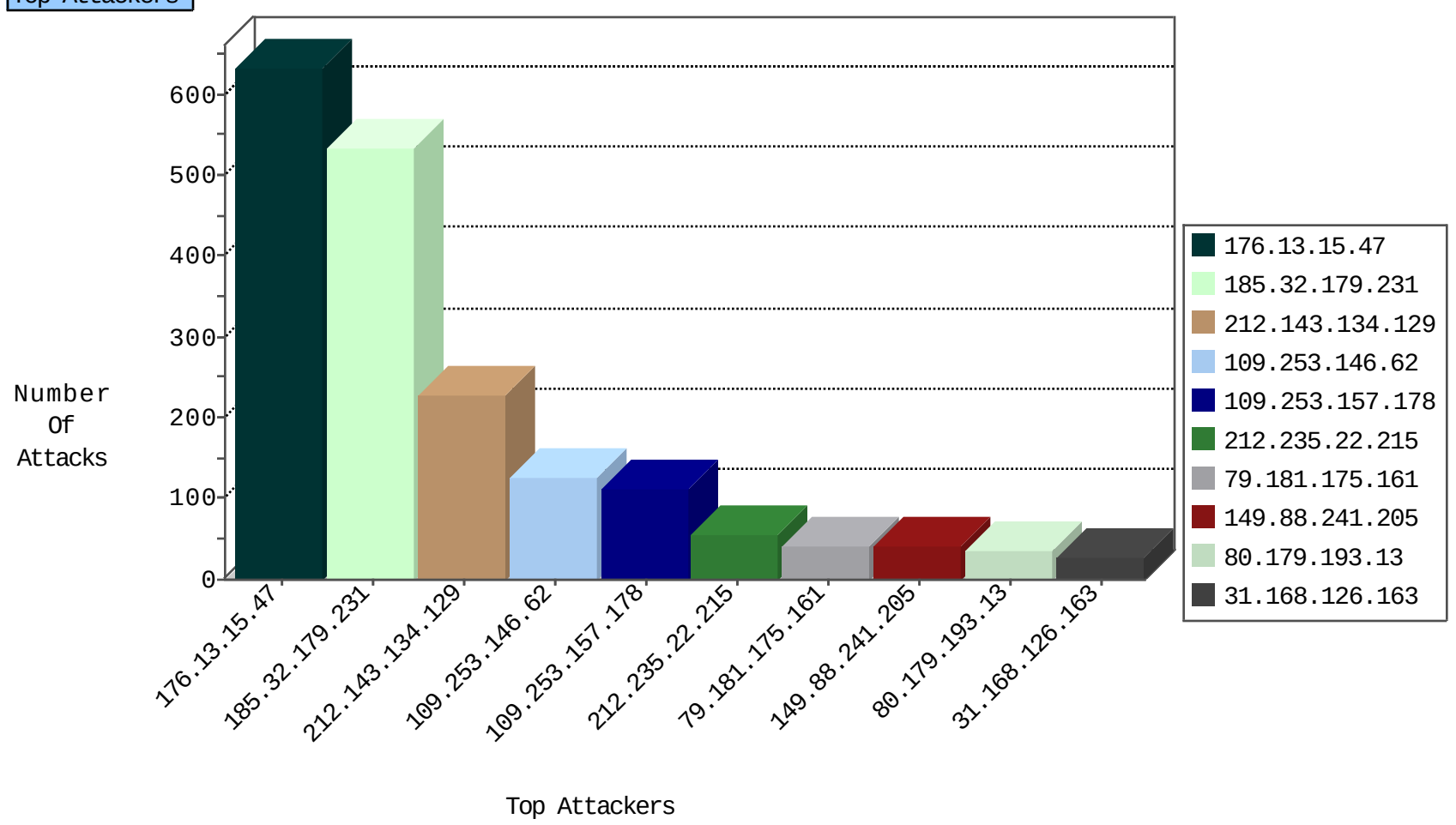
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.50.138	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	24
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
83.22.76.18	Poland	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.76.174.2	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Top Attackers In IDS

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

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	228
212.235.22.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
31.168.126.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
149.88.241.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
93.172.144.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.54.135.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.253.146.62	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
81.218.173.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
213.8.41.145	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.102	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.131.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.153.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.61.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.63.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.180.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.110.40.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.25.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.176	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.154.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.204.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.8.118	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.196.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.250	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.146	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
89.108.144.114	Lebanon	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.102	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.49.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.237.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.182.191.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.64.144.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.135.147	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
82.81.18.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.147.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.239.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.112.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.123.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.127.228.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-09-2016-14:04:00 to 02-09-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	307
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	208
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	115
109.253.146.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
109.253.157.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	100
80.179.193.13	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.179.193.13	Block	36
109.253.201.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
2.54.53.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.54.3.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
149.88.241.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
37.26.148.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.137.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
93.172.144.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
184.154.233.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
62.90.214.50	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
109.253.157.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.3.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.228.255.144	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.12.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.186.185.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
2.54.39.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.140.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
94.100.245.126	Germany	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	2
2.54.2.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/	Block	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.181.175.161	Block	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
185.109.163.5		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.80	Block	1
37.26.149.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
80.246.137.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.79.127	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
178.44.51.25	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3333.pdf	Block	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.181.175.161	Block	1
46.19.85.218	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Accept-Language: in URL he-il,he	Block	1
109.64.81.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version drkP{ÃŸÃšzÃ'uÃ–RÃ-Â,Ã¼SQÂ€ÂœÃ¿Ã§MrÂ²Ã†sÃ™ .DÂ¦[[#0]]&Ã»v! Â·}RÂ"Ã?[[#17]]Ã³Â–Â"Ã‹LÂ±[[#31]][[#18]]Ã"Ã LÃ±Â‰ 4(2?[[#31]]f[[#23]][[#30]]Ã—Ã–Ã²N9ÂƒBÃ•v[[#22]]Ã®:[[#6]]Âƒ [[#7]]Â°[[#27]]YÃ›2OÃ´[[#20]][[#7]]Â³Ã-Ã¶Â›Â§EÂ†qE[[#23]]=t3cy3IÂƒ Â»ÃµoÃ·[[#24]]'1Ã‡Ã‰FÂŸgl\>!+ÂŠÂ…Â?5?Â¦Â¹Ã›Ã"Â¼Ã,Â¯Â£"[[#19]]Â“ &Ã„rÃŠÂ¶	Block	1
79.180.155.208	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/109622.pdf	Block	1
176.13.17.203	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
36.250.168.7	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.181.175.161	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.181.175.161	Block	1
62.219.54.250	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

02-09-2016-14:04:00 to 02-09-2016-15:04:00