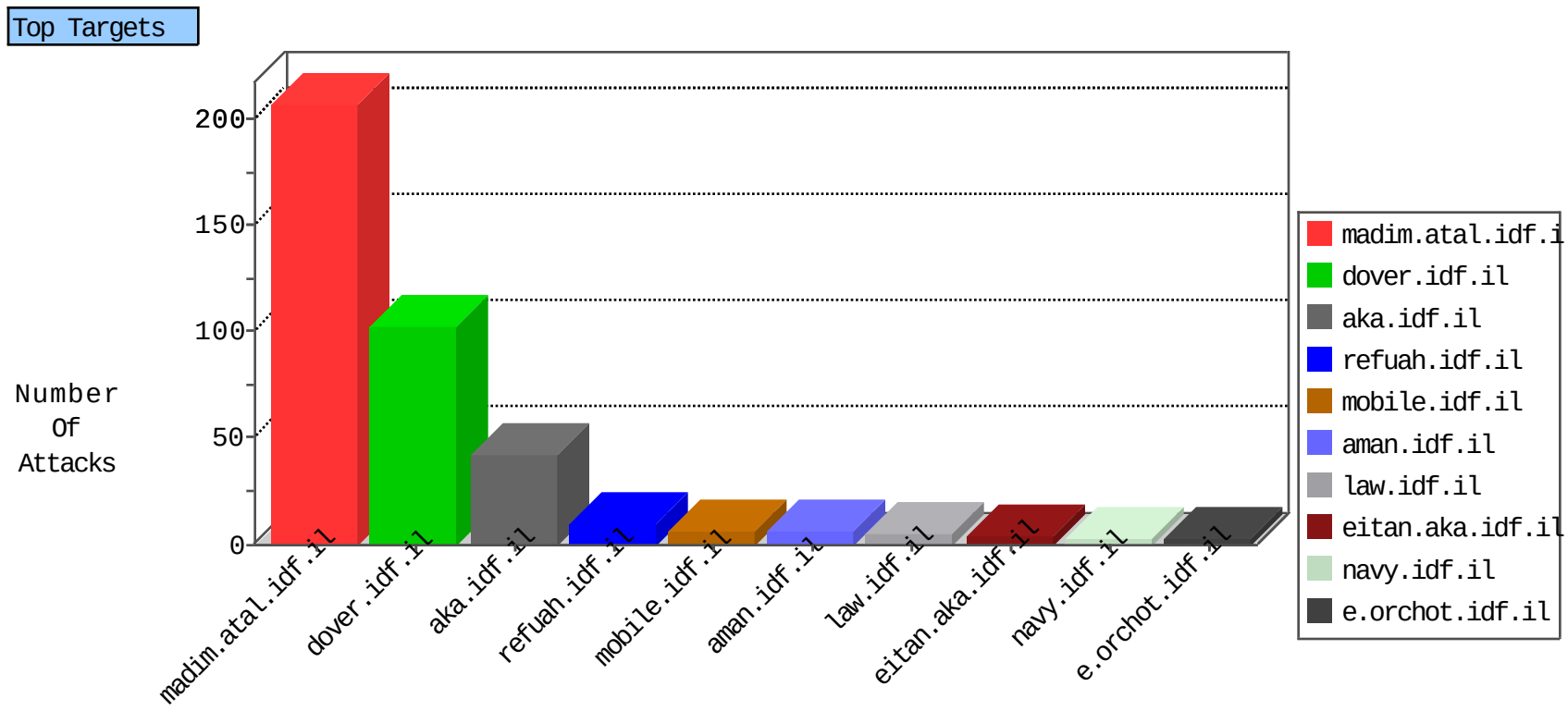
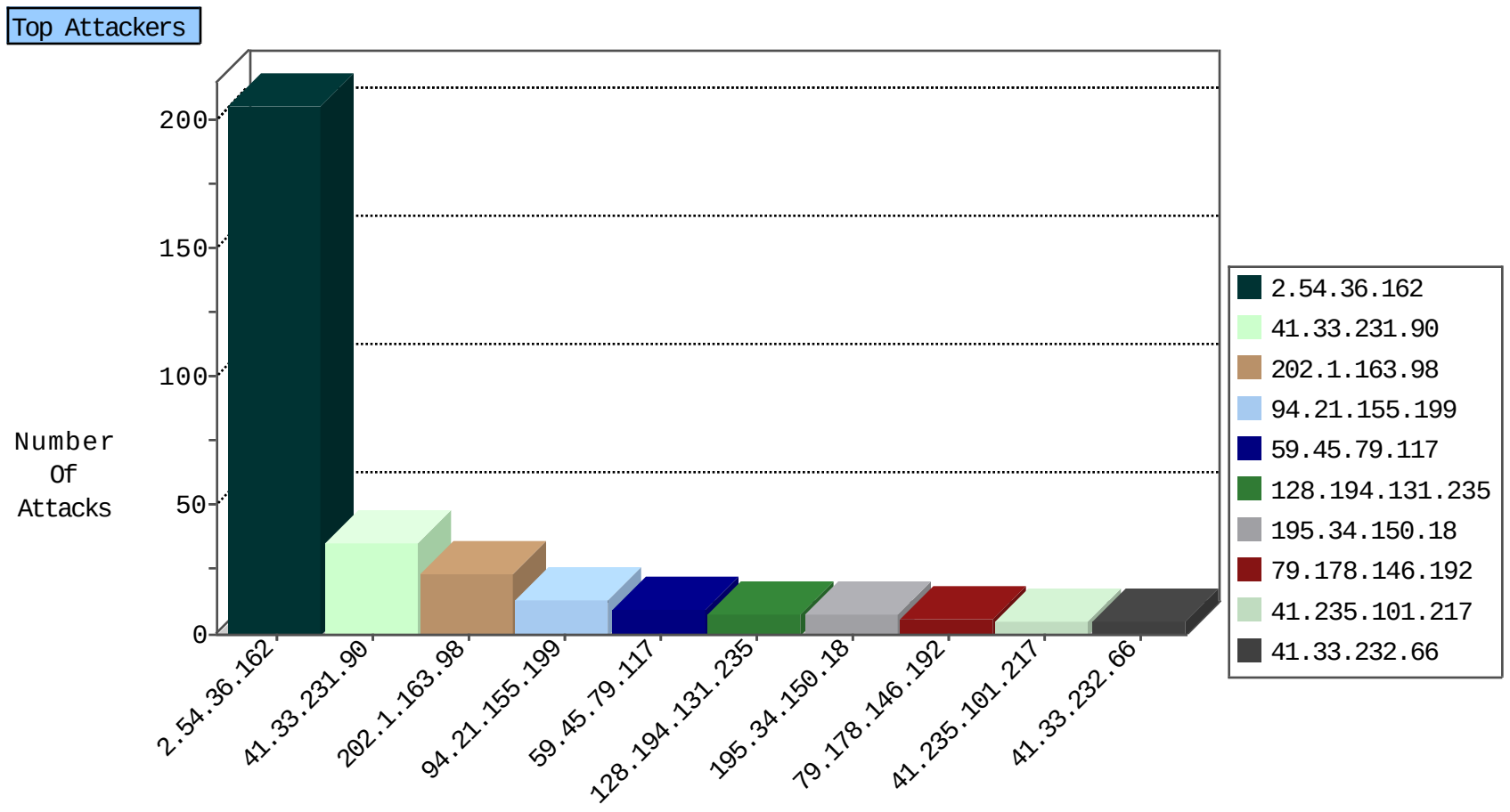
02-09-2016-02:04:04 to 02-09-2016-03:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-09-2016-02:04:04 to 02-09-2016-03:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.58	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
74.91.28.60	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
142.54.160.212	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
142.54.169.164	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

02-09-2016-02:04:04 to 02-09-2016-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.245.194.62	Latvia	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

02-09-2016-02:04:04 to 02-09-2016-03:04:04

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	4
66.249.74.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.31	United States	nakchal.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
194.187.249.70	147.237.77.74	Europe	law.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
1.54.210.107	147.237.77.216	Vietnam	dover.idf.il	ET SCAN NMAP -sS window 3072	1
104.197.96.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.31		nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
211.149.187.104	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.240	147.237.76.177		ncore.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.165	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.54.210.107	147.237.77.216	Vietnam	dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

02-09-2016-02:04:04 to 02-09-2016-03:04:04

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
202.1.163.98	Solomon Islands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
79.178.146.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
41.235.101.217	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.132.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.197.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.192.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.223.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.158.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.24.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.29.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.144.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
66.249.75.37	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
68.52.222.67	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.131.0	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.81.38.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.43	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
155.94.254.143	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
210.50.41.76	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
178.62.162.228	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.52.222.67	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.177.106.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.63.97.227		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
180.76.15.140	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-09-2016-02:04:04 to 02-09-2016-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.36.162	Block	83
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL Â qâ€ºÖ±%×–;Â´Ã¿â€¡%[[#24]]× Ë†Â¨×œ [[#25]][[#8]]Ã·bÂ·__Ö±×–lziÆ’6[[#19]][[#14]]Ã·[[#16]]×§×³[[#11]]k×¦:o	Block	1
66.249.79.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kapaz/contactus.asp	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	NULL Character in Header Name at Ã¢MÃ„zÂ„[[#31]]%[[#14]]~Â¨Ã¯	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
202.1.163.98	Solomon Islands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sharebsite	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal HTTP Version ÂµÃ€Â¸ Â„Â€#'@[[#25]]Ã®EÂ´8ÂŽ+Â,f$[[#17]]Â?ÂˆÃ•Ã‡ Â½[[#12]]Ã£ÃŽ=U]Ã°RrHÂ”Ã?Ã®;PÂˆÂ•Â¦Â¤Ã¯[[#1]]Â¤Ã¿Ã¡ÂžP[[#1]]4Z8n*<mÂˆrFÃž[[#23]]Â‡[[#31]]pIÂ,6]Â¥Ã¡[[#27]][[#24]]I)i5Â‘Ã´ÃŒÂ”'5Ãª~Â³Â-.d=^Ã–Â…gÃ‰a7ÂœÃ©Iu[[#31]]Ã,Ã¼Â-Â»Â†Â†Ã?Ã† +DÃ?[[#11]]4Ã¡Ã·Ã©rÂ¥9Â‰Ã¦ Ã¸Ã€[[#16]]Â“[[#19]]Â?Ã‹(Ãª:cÂ…$[[#19]]Ã’ Ã›Ã„3Â³lo"{Â°Â°ÂœjPM?Âµ.^Ã‹ÃŒÃ¾Â“wlÂ¸ÂžÂ<(ÂŽ[[#22]]Â–Â¼ul.Â?8[[#31]]fÂ·[[#18]]sÃšÑÃªÂŽ}Â®Ã¿Ã•Ã?Â²_Â‹b)[[#23]]ÂŠÃ¤Â¦[[#28]]Ã§Â”Ã¼Ã½Ã°QÃ-%Â?	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Too Many Headers per Request - 37 Headers	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	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/0/2400.jpg	Block	1
208.115.113.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal URL Path Encoding Â qâ€ºÖ±%×–;Â´Ã¿â€¡%[[#24]]× Ë†Â¨×œ [[#25]][[#8]]Ã·bÂ·__Ö±×–lziÆ’6[[#19]][[#14]]Ã·[[#16]]×§×³[[#11]]k×¦:o	Block	1
84.228.147.213	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Unknown HTTP Request Method yÂ±uÂ›[[#22]]/Â±ÃºÂ?Â‰Â§Âª'wR,Â¯;Ã…Ã’ [[#28]]%E9[[#3]]pu[[#16]]RÃ«Â»_XU]=Â-hE	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2808.jpg	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 21	Block	1
84.228.147.213	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method yÂ±uÂ›[[#22]]/Â±ÃºÂ?Â‰ Â§Âª'wR,Â¯;Ã…Ã’[[#28]]%E9[[#3]]pu[[#16]]RÃ«Â»_XU]=Â-hE	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Malformed URL Â qâ€ºÖ±%×–;Â´Ã¿â€¡%[[#24]]× Ë†Â¨×œ [[#25]][[#8]]Ã·bÂ·__Ö±×–lziÆ’6[[#19]][[#14]]Ã·[[#16]]×§×³[[#11]]k×¦:o	Block	1
94.21.155.199	Hungary	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
157.55.39.48	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1

02-09-2016-02:04:04 to 02-09-2016-03:04:04