İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329936537)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329936538)

[ÖRNEK PARSING 4](#_Toc329936539)

[TEMEL PARSING YAPISI 5](#_Toc329936540)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 12.06.2013 | V\_1 | Eski recorder parser yapmadığı için geliştirme istendi | Fatih Sakar |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | TrendMicroBlockUrl |
| Versiyonu | - |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | TrendMicroURLBlockSyslogV\_1Recorder |
| İstek yapan Adı Soyadı | Fatih sakar |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 12.06.2013 |
| İstek yapılan kurum adı | TSE |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | - |
| İlişkili form adı | - |
| Servis Yetkilisi Notları | - |
| Geliştirici Notları | - |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 10.6.1.80:52898 : local0.critical proxy.tse.tr: <Wed, 12 Jun 2013 11:25:46,EEST> [EVT\_URL\_BLOCKING|LOG\_CRIT] Blocked URL log tk\_username=10.34.3.56,tk\_date\_field=2013-06-12 11:25:46+0300,tk\_protocol=http,tk\_url=http://tools.google.com/googletalk/google-talk-versioncheck-tr.txt?auv=1&amp:r=4&amp:up=30&amp:p=w&amp:ma=6&amp:mi=1&amp:b=7601&amp:sp=ServicePack1&amp:as=googletalk&amp:pv=1.0.0.105,tk\_malicious\_entity=,tk\_file\_name=,tk\_entity\_name=,tk\_action=,tk\_scan\_type=content filter,tk\_blocked\_by=policy,tk\_rule\_name=TSE,tk\_opp\_id=0,tk\_group\_name=None,tk\_category=Software Downloads,tk\_uid=0013090619-71f3e6e312730a5beeac,tk\_filter\_action=1 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME |  |
| SOURCENAME | 10.6.1.80 |
| EVENTCATEGORY | http |
| EVENTTYPE | Blocked URL |
| USERSID | 10.34.3.56 |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | tools.google.com |
| CUSTOMSTR2 | <http://tools.google.com/googletalk/google-talk-versioncheck-tr.txt?auv=1&amp:r=4&amp:up=30&amp:p=w&amp:ma=6&amp:mi=1&amp:b=7601&amp:sp=ServicePack1&amp:as=googletalk&amp:pv=1.0.0.105,tk_malicious_entity=,tk_file_name=,tk_entity_name=,tk_action=,tk_scan_type=content> |
| CUSTOMSTR3 | 10.34.3.56 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 | Software Downloads |
| CUSTOMSTR6 | 0013090619-71f3e6e312730a5beeac |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | TSE |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |