İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
|  |  |  |  |
| 07.09.2013 | 1 | TrendMicroInterScanWebGatewayRecorder | Ali BOZDAĞ |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | TrendMicroInterScanWebGatewayRecorder |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | TrendMicroInterScanWebGatewayV\_1\_0\_0Recorder |
| İstek yapan Adı Soyadı | Ali BOZDAĞ |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 07.09.2013 |
| İstek yapılan kurum adı | KALKINMA BAKANLIĞI |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları | EVENTTYPE Blocked URL log ve Access tracking log olmayanlarda alıcanaktır. Diğer loğlar description kolonuna basılacaktır. |

# NOT:

Full log’un description alanına basılması gerekmektedir.

# ÖRNEK PARSING - I

|  |  |
| --- | --- |
| 10.20.1.122:9476 : local0.info iwsva1.dpt.gov.tr: <Fri, 06 Sep 2013 15:32:35,EEST> [EVT\_URL\_ACCESS\_TRACKING|LOG\_INFO] Access tracking log tk\_username=10.12.1.255,tk\_url=http://www2.sporx.com/\_img/footer/dikey\_ayrac.gif,tk\_size=57,tk\_date\_field=2013-09-06 15:32:35+0300,tk\_protocol=http,tk\_mime\_content=image/gif,tk\_server=iwsva1.dpt.gov.tr,tk\_client\_ip=10.12.1.255,tk\_server\_ip=77.223.146.114,tk\_domain=www2.sporx.com,tk\_path=\_img/footer/dikey\_ayrac.gif,tk\_file\_name=dikey\_ayrac.gif,tk\_operation=GET,tk\_uid=0678949940-c9cb8c872d05a9f77212,tk\_category=65,tk\_category\_type=0 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2013-09-06 15:32:35+0300 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | Access tracking log |
| USERSID | 10.12.1.255 |
| LOGNAME |  |
| COMPUTERNAME | iwsva1.dpt.gov.tr |
| CUSTOMSTR1 | GET |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.12.1.255 |
| CUSTOMSTR4 | 77.223.146.114 |
| CUSTOMSTR5 | http |
| CUSTOMSTR6 | image/gif |
| CUSTOMSTR7 | www2.sporx.com |
| CUSTOMSTR8 | \_img/footer/dikey\_ayrac.gif |
| CUSTOMSTR9 | 0678949940-c9cb8c872d05a9f77212 |
| CUSTOMSTR10 | http://www2.sporx.com/\_img/footer/dikey\_ayrac.gif |
| CUSTOMINT1 | 57 |
| CUSTOMINT2 | 65 |
| CUSTOMINT3 | 0 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |
|  |  |

# ÖRNEK PARSING - II

|  |  |
| --- | --- |
| 10.20.1.122:9476 : local0.critical iwsva1.dpt.gov.tr: <Fri, 06 Sep 2013 16:43:37,EEST> [EVT\_URL\_BLOCKING|LOG\_CRIT] Blocked URL log tk\_username=10.14.1.136,tk\_date\_field=2013-09-06 16:43:37+0300,tk\_protocol=http,tk\_url=http://www.turkcellsohbethatlari.net/wp-content/uploads/Canli-Sohbet-Telefonu.jpg,tk\_malicious\_entity=,tk\_file\_name=,tk\_entity\_name=,tk\_action=,tk\_scan\_type=content filter,tk\_blocked\_by=policy,tk\_rule\_name=Kalkinma\_policy,tk\_opp\_id=0,tk\_group\_name=None,tk\_category=Adult/Mature Content,tk\_uid=0683244535-ecbc2b2f92b4f430db57,tk\_filter\_action=1 | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2013-09-06 16:43:37+0300 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | Blocked URL log |
| USERSID | 10.14.1.136 |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 | www.turkcellsohbethatlari.net |
| CUSTOMSTR2 | http://www.turkcellsohbethatlari.net/wp-content/uploads/Canli-Sohbet-Telefonu.jpg |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 | http |
| CUSTOMSTR6 | content filter |
| CUSTOMSTR7 | policy |
| CUSTOMSTR8 | Kalkinma\_policy |
| CUSTOMSTR9 | 0683244535-ecbc2b2f92b4f430db57 |
| CUSTOMSTR10 | Adult/Mature Content |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 | 0 |
| CUSTOMINT6 | 1 |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |