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 |
|  |  |  |  |
| 26.12.2012 | 1 | Hotspot Recorder | Kaan Emre KOŞAR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | CryptTechHotspotRecorder |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi |  |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 26.12.2012 |
| İstek yapılan kurum adı | TEİAŞ |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | /var/log/nateklog/natek\_20121212.log |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları | Bu formatta olmayan satırlar alınmayacak, bilgileri eksik olsada bu formatta olan satırlar aynı şekilde alınacaktır. |

# NOT:

Customstr1 ve Customstr2 kolonlarında 900 kontrolu yapılmasında fayda var. Ayrıca full log’un description alanına basılması gerekmektedir.

# ÖRNEK PARSING - I

|  |  |
| --- | --- |
| Nov 3 19:42:08 clog logger: 10.10.1.23 - - [03/Nov/2012:19:42:08 +0200] "POST http://10.10.1.1/cryptospot/login/login.php?res=notyet&uamip=10.10.1.1&uamport=3100&challenge=16876269efa03abd1d8a48d4fdcc1a34&called=00-25-90-34-BF-2B&mac=00-E0-4C-81-91-A4&ip=10.10.1.23&nasid=nas-10&sessionid=509557090000000e&userurl=http%3a%2f%2fwww.cnn.com%2f&md=EA8267CFBC2E9896C5A067F5C64DC9B7 HTTP/1.1" - - "http://10.10.1.1/cryptospot/login/login.php?res=notyet&uamip=10.10.1.1&uamport=3100&challenge=16876269efa03abd1d8a48d4fdcc1a34&called=00-25-90-34-BF-2B&mac=00-E0-4C-81-91-A4&ip=10.10.1.23&nasid=nas-10&sessionid=509557090000000e&userurl=http%3a%2f%2fwww.cnn.com%2f&md=EA8267CFBC2E9896C5A067F5C64DC9B7" "Mozilla/5.0 (Linux; U; Android 4.0.4; tr-tr; P079R Build/IMM76D) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Safari/534.30" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 03/Nov/2012:19:42:08 +0200 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | POST |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | 10.10.1.23 |
| CUSTOMSTR1 | http://10.10.1.1/cryptospot/login/login.php?res=notyet&uamip=10.10.1.1&uamport=3100&challenge=16876269efa03abd1d8a48d4fdcc1a34&called=00-25-90-34-BF-2B&mac=00-E0-4C-81-91-A4&ip=10.10.1.23&nasid=nas-10&sessionid=509557090000000e&userurl=http%3a%2f%2fwww.cnn.com%2f&md=EA8267CFBC2E9896C5A067F5C64DC9B7 |
| CUSTOMSTR2 | http://10.10.1.1/cryptospot/login/login.php?res=notyet&uamip=10.10.1.1&uamport=3100&challenge=16876269efa03abd1d8a48d4fdcc1a34&called=00-25-90-34-BF-2B&mac=00-E0-4C-81-91-A4&ip=10.10.1.23&nasid=nas-10&sessionid=509557090000000e&userurl=http%3a%2f%2fwww.cnn.com%2f&md=EA8267CFBC2E9896C5A067F5C64DC9B7 |
| CUSTOMSTR3 | HTTP/1.1 |
| CUSTOMSTR4 | Mozilla/5.0 (Linux; U; Android 4.0.4; tr-tr; P079R Build/IMM76D) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Safari/534.30 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |

# ÖRNEK PARSING - II

|  |  |
| --- | --- |
| Dec 11 07:58:28 clog logger: 10.10.1.19 - - [11/Dec/2012:07:58:28 +0200] "GET http://gfx1.hotmail.com/mail/w4/pr04/ltr/net\_up.gif?r=0.9213891135431961&d=1355205377304&t=0 HTTP/1.1" - - "http://co122w.col122.mail.live.com/default.aspx?rru=inbox" "Mozilla/5.0 (Windows NT 5.1; rv:17.0) Gecko/20100101 Firefox/17.0" | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 11/Dec/2012:07:58:28 +0200 |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE | GET |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | 10.10.1.19 |
| CUSTOMSTR1 | http://gfx1.hotmail.com/mail/w4/pr04/ltr/net\_up.gif?r=0.9213891135431961&d=1355205377304&t=0 |
| CUSTOMSTR2 | http://co122w.col122.mail.live.com/default.aspx?rru=inbox |
| CUSTOMSTR3 | HTTP/1.1 |
| CUSTOMSTR4 | Mozilla/5.0 (Windows NT 5.1; rv:17.0) Gecko/20100101 Firefox/17.0 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Full Log |