Giriş

DocGuard-Watcher Nedir

DocGuard Watcher , DocGuard Api yardımı ile Office, PDF ve HTA gibi dökümanlar içerisindeki zararlı yazılım aktivitelerini yapısal olarak analiz edip tespit eden bir endpoint uygulamasıdır.

DocGuard-Watcher işletim sistemi içerisinde “windows service” olarak çalışır. Görevleri arasında İşletim sistemi içerisinde gerçekleşen File I/O (Dosya yazma, oluşturma , güncelleme ve isim değiştirme vs.) işlemlerini Windows Callback yapısını kullanarak takip etmek ve daha sonra ilgili dosyayı taranması için DocGuard’da gönderip elde ettiği sonucu Windows Event Log içerisine yazmaktır. Herhangi bir arayüze sahip olmayan bu servis sayesinde endpoint üzerinde gerçekleşen döküman dosyalarına ait aktiviteler otomatik olarak “Olay Günlüğü” altında kayıt altına alınacak ve Siem, EDR gibi uygulamalar tarafından kullanılabilir olacaktır.

Event Log Kayıt tipleri

DocGuard-Watcher kendi içerisinde 3 farklı Event Log kayıt tipi vardır. Bu tipler içerisinde Warning mesajları default olarak kapalı gelir.

1. **Information Log** : Bu kayıt tipi DocGuard-Watcher tarafından service başlatma, durdurma ve analize gönderilen dosyanın analiz çıktısı için kullanılır. Event ID numarası 10000 dir.
2. **Warning Log** : Bu kayıt tipi DocGuard-Watcher çalışırken uygulama tarafında exception’a düşen durumlar için kullanılır. Event ID numarası 10001 dir.
3. **Error Log** : Registery-Path’in olmaması , girilen credentials’ların geçerli olmaması ve internet erişim sorunu olduğunda kullanılan formattır. Event ID numarası 10002 dir.

Desteklenen uzantılar

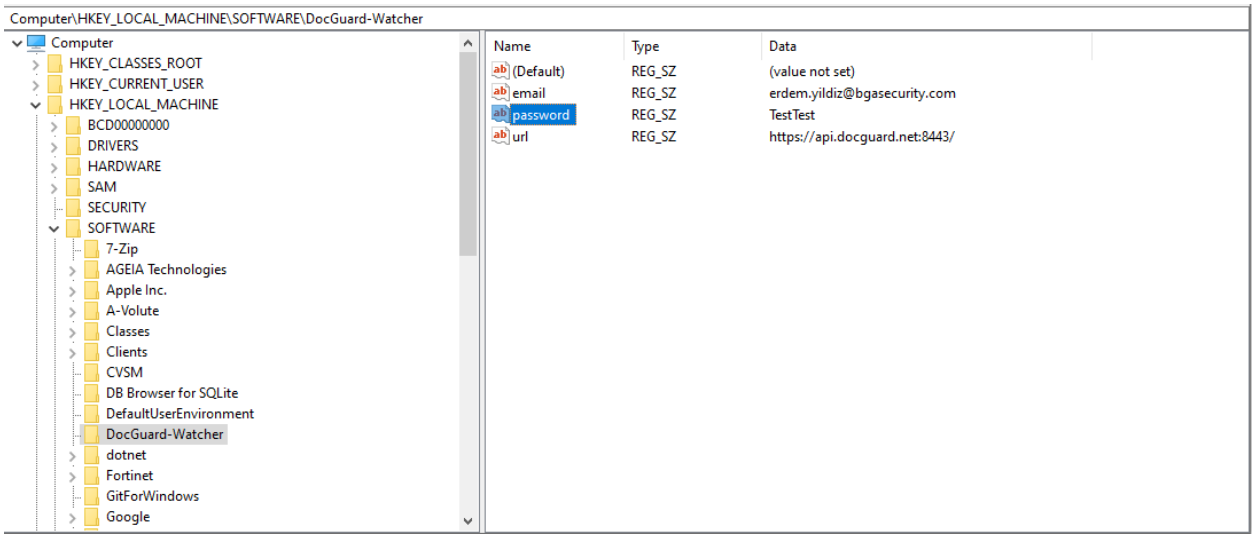
- .hta
- .pdf
- .slk
- .csv
- .doc
- .dot
- .docx
- .docm

- .dotx
- .dotm
- .wll
- .xls
- .xll
- .xlw
- .xlt
- .xlsx
- .xlsm
- .xlsb
- .xlam
- .xltx
- .xltm
- .ppt
- .pps
- .pptx
- .pptm
- .ppsx
- .ppam
- .ppa
- .rtf
- .bin
- .pub

Kurulum

Registry

“Computer\HKEY_LOCAL_MACHINE\SOFTWARE\” altında DocGuard-Watcher isimli key oluşturup içerisine “email”,”password” ve “url” alanların eklenmesi gerekmektedir.



- email = “”
- password =””
- url = “https://api.docguard.net:8443/”

Service oluşturma

Windows içerisinde DocGuard-Watcher service’ini oluşturmak için aşağıdaki gibi bir komutlardan size uygun olanı kullanabilirsiniz.

Normal şekilde service oluşturmak için aşağıdaki komut kullanılabilir.

- sc create DocGuard-Watcher binpath="C:\Path\DocGuard-Watcher.exe"

Eğer EventLog’lar içerisinde warning mesajlarının görülmesi isteniyorsa komut aşağıdaki gibi olmalıdır.

- sc create DocGuard-Watcher binpath="C:\Path\DocGuard-Watcher.exe --warning"

Notlar

- DocGuard-Watcher, Default kurulumda dosyalarınızı DocGuard Api servisine public olacak şekilde işaretleyerek gönderir. Bu, analiz sonuçlarının diğer kullanıcılar tarafından da görülebilir olduğunu ifade eder. Şayet sadece profilinize özel Private bir analiz istiyorsanız https://app.docguard.io üzerinden uygulamaya üye olmalı ve üyelik bilgilerinizi Registry anahtarı altındaki değerlere yazmalısınız.
- **Gizlilik**: DocGuard uygulaması dosyalarınızla ilgilenmez. Dosyalarınız analiz edildikten sonra belirli bir periyod da otomatik olarak silinir ve sadece analize uygun metadata ve

analiz sonuçları veritabanına yazılarak saklanır. Gizlilik konusunda hassasiyeti olan firmalar için DocGuard ayrıca kurum sistemlerine Docker ile kolayca deploy edilebilir. Bunun için https://docguard.io üzerinden iletişime geçebilirsiniz.