

USB를 통해 지속적으로 유포 중인 코인 마이너 악성코드

A asec.ahnlab.com/ko/91280

ATCP

November 27, 2025



AhnLab SEcurity intelligence Center(ASEC)은 2025년 2월 “USB로 전파되는 암호화폐 채굴 악성코드 유포 사례”[\[1\]](#) 보고서를 통해 국내에 코인 마이너 악성코드가 USB를 통해 전파 중인 것을 확인하였다. 2025년 7월에는 Mandiant에서도 동일한 공격 사례를 공개하였으며 설치되는 악성코드들을 DIRTYBULK, CUTFAIL 등으로 분류하였다. [\[2\]](#)

전체적인 공격 방식은 크게 변하지 않았지만 기존 유형과 비교해서 최근에는 새로운 유형의 악성코드가 사용되고 있으며 여기에서는 최신 악성코드들을 기준으로 분석한다.

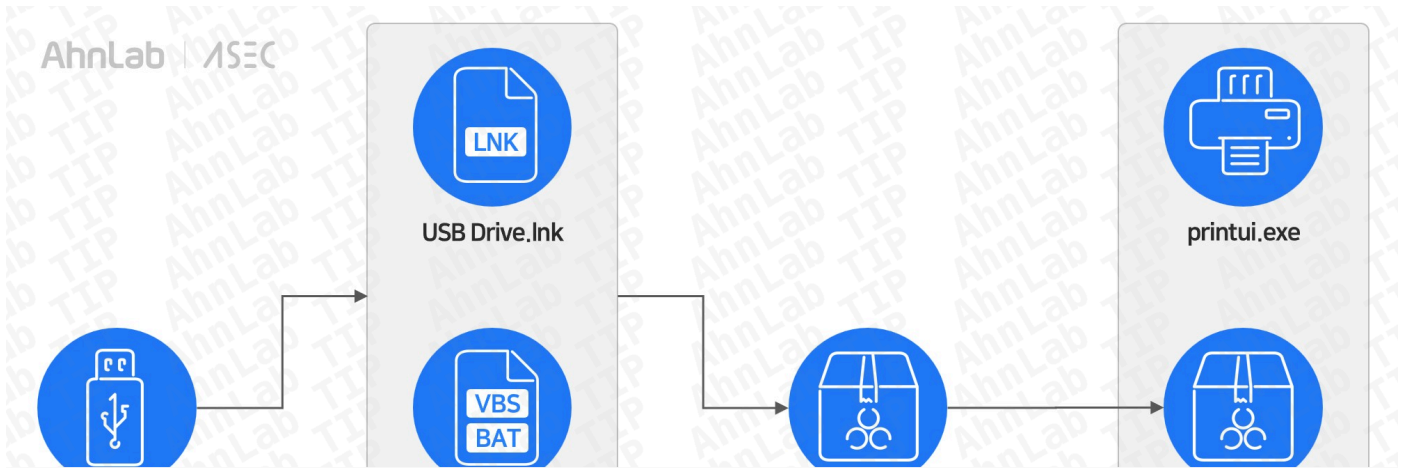


Figure 1. 흐름도

1. USB를 통한 전파

감염된 USB는 다음과 같이 “USB Drive.lnk” 파일이 보여지며 이외에도 “sysvolume”, “USB Drive” 폴더들이 숨김 속성으로 존재한다. “폴더 옵션”의 “보기” 탭에서 “숨김 파일, 폴더 및 드라이브 표시”를 선택하면 숨겨진 폴더 “sysvolume”와 “USB Drive”를 확인할 수 있다.

일반적으로 사용자가 USB 삽입 후 해당 화면을 보게 되면 “USB Drive.lnk” 파일을 더블 클릭하여 실행하게 될 것이다. “USB Drive.lnk” 바로 가기 파일은 “sysvolume” 폴더에 존재하는 “u566387.vbs”와 같이 “u”로 시작하는 랜덤한 6개의 숫자를 이름으로 갖는 VBS 악성코드를 실행한다.

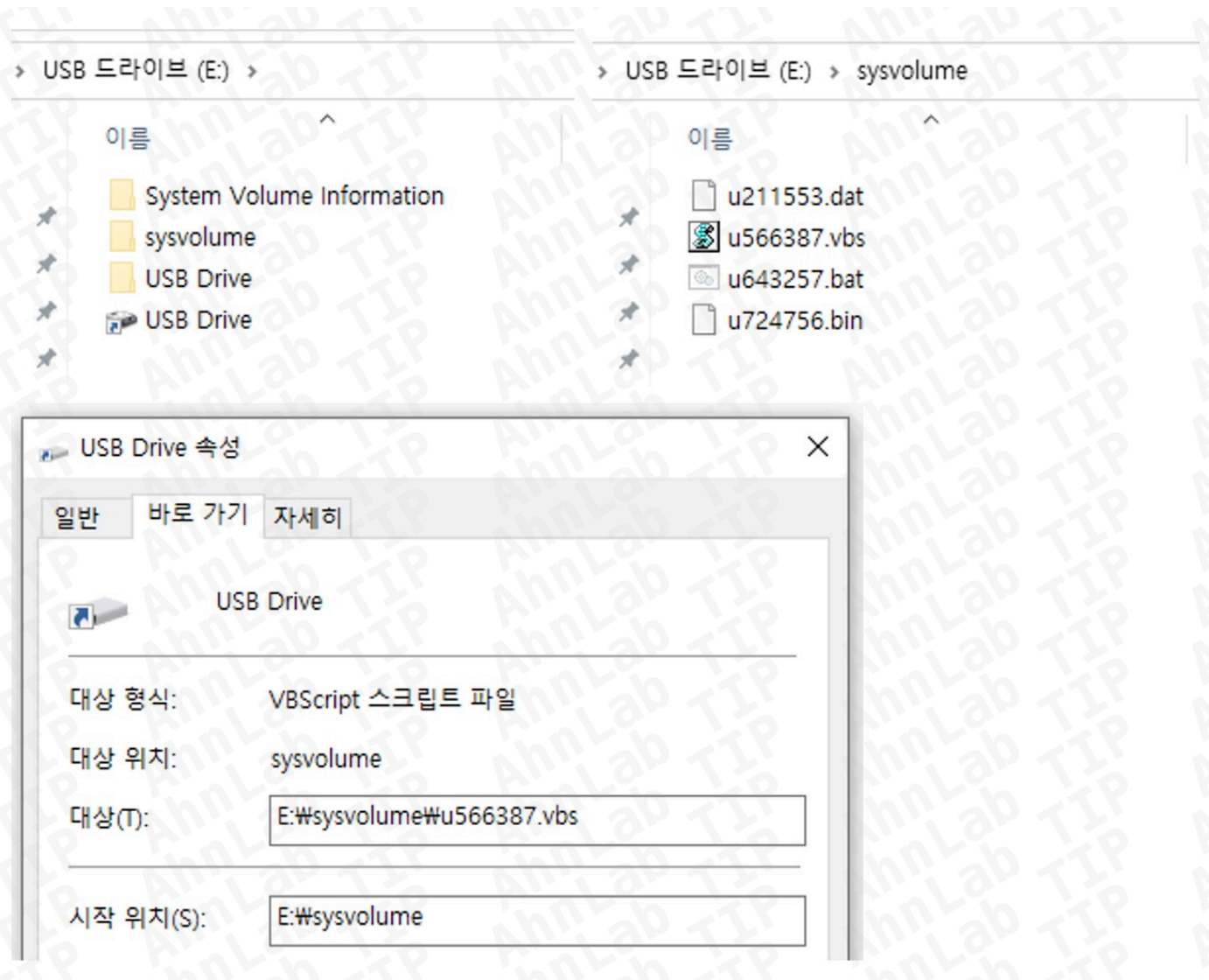


Figure 2. 감염된 USB 내의 파일들

VBS 악성코드는 동일 경로에 있는 “u643257.bat”와 같은 이름의 BAT 악성코드를 실행하는 기능을 담당한다. BAT 악성코드는 “USB Drive” 폴더를 오픈하는데 해당 폴더에는 USB에 포함되어 있던 원본 파일들이 존재한다. 이에 따라 사용자는 정상적으로 USB를 사용할 수 있으며 악성코드 감염 정황을 파악하기 어려울 수 있다. 참고로 BAT 악성코드는 이외에도 “C:\Windows\System32\”와 같은 공백이 포함된 폴더를 생성하고 드로퍼 악성코드인 “u211553.dat”을 “printui.dll”이라는 이름으로 복사한다. 그리고 “%SystemDirectory%” 폴더에 존재하는 “printui.exe” 파일을 “C:\Windows\System32\” 폴더에 복사한 후 실행하여 악성코드인 “printui.dll” 즉 “u211553.dat”가 정상 프로그램인 “printui.exe”에 로드되어 실행될 수 있도록 한다.

```

If Not WScript.Arguments.Named.Exists("elevated") Then
    Set sh = CreateObject("Shell.Application")
    sh.ShellExecute "wscript.exe", Chr(34) & WScript.ScriptFullName & Chr(34) & " /elevated",
        "", "runas", 1
    WScript.Quit
End If
Set fs = CreateObject("Scripting.FileSystemObject")
pp = fs.GetParentFolderName(WScript.ScriptFullName)
bp = pp & "\u643257.bat"
If fs.FileExists(bp) Then

```

Figure 3. 악성코드 설치 스크립트들

2. 드로퍼

“printui.dll”는 드로퍼 악성코드로서 내부에 존재하는 또 다른 악성코드를 “%SystemDirectory%\svcinsty64.exe” 경로에 생성하고 실행하는 기능을 담당한다. “svcinsty64.exe” 또한 드로퍼로서 “%SystemDirectory%\svctrl64.exe” 파일을 생성하고 실행하며 이외에도 설정 파일인 “wlogz.dat”를 “%SystemDirectory%\wsvcz” 폴더에 생성한다. 이후 자식 프로세스로서 “svctrl64.exe”를 실행한다.

“svctrl64.exe” 또한 드로퍼인데 최종적으로 “%SystemDirectory%” 폴더에 “u826437.dll”와 같은 이름의 DLL을 생성하고 DcomLaunch 서비스에 등록한다.

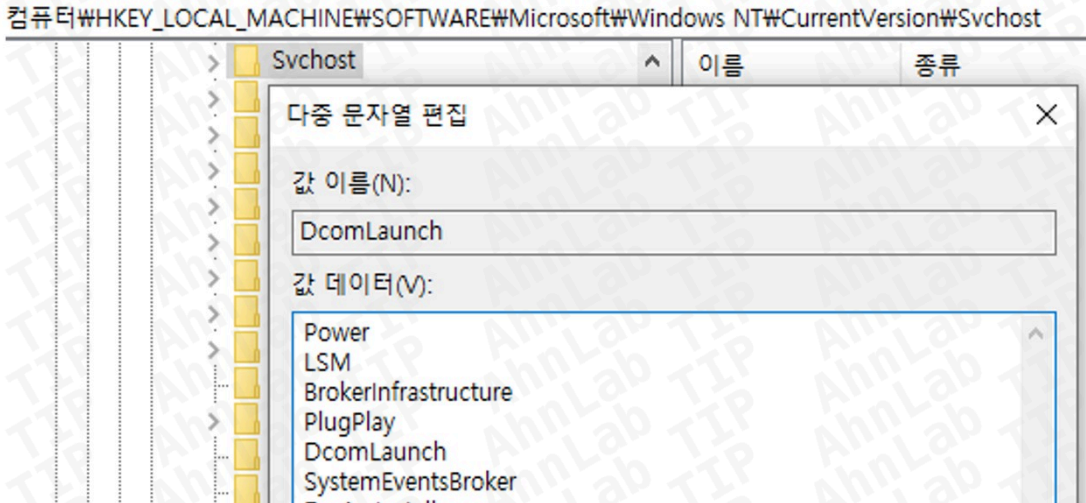


Figure 4. DcomLaunch 서비스에 등록된 악성코드

3. PrintMiner

DcomLaunch 서비스에 의해 실행되는 악성코드는 분류를 위해 PrintMiner로 정리한다. PrintMiner는 윈도우 디펜더에 설치 경로를 예외 폴더로 등록하고 전원 설정을 조정하여 시스템이 대기 모드로 전환되지 않도록 한다. 이후 C&C 서버의 주소를 구하고 CPU, GPU 등 감염 시스템의 정보를 전송한다. 여기까지의 과정이 끝나면 "%SystemDirectory%\wsvcz" 폴더에 XMRig를 포함한 추가적인 페이로드를 설치하는데 다운로드된 파일들은 암호화되어 있기 때문에 복호화하는 과정이 함께 진행된다.

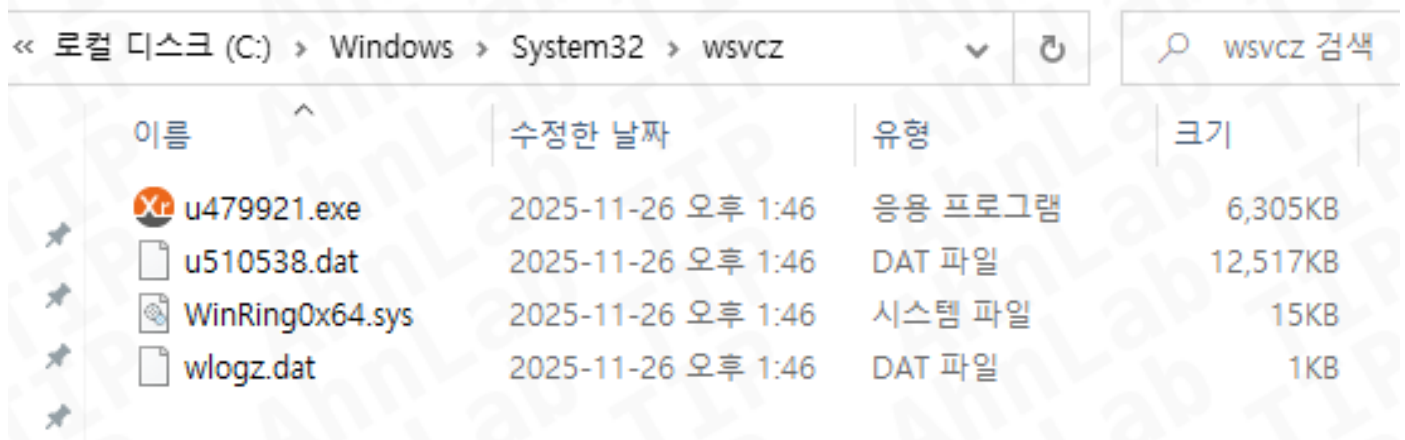


Figure 5. 복호화된 설치 파일들

참고로 “%SystemDirectory%\wsvcz\wlogz.dat” 경로에 위치하는 설정 파일은 다음과 같이 C&C 서버의 IP 주소, 마이닝 정보, 설치된 악성코드 경로 등의 정보가 포함되도록 업데이트된다.

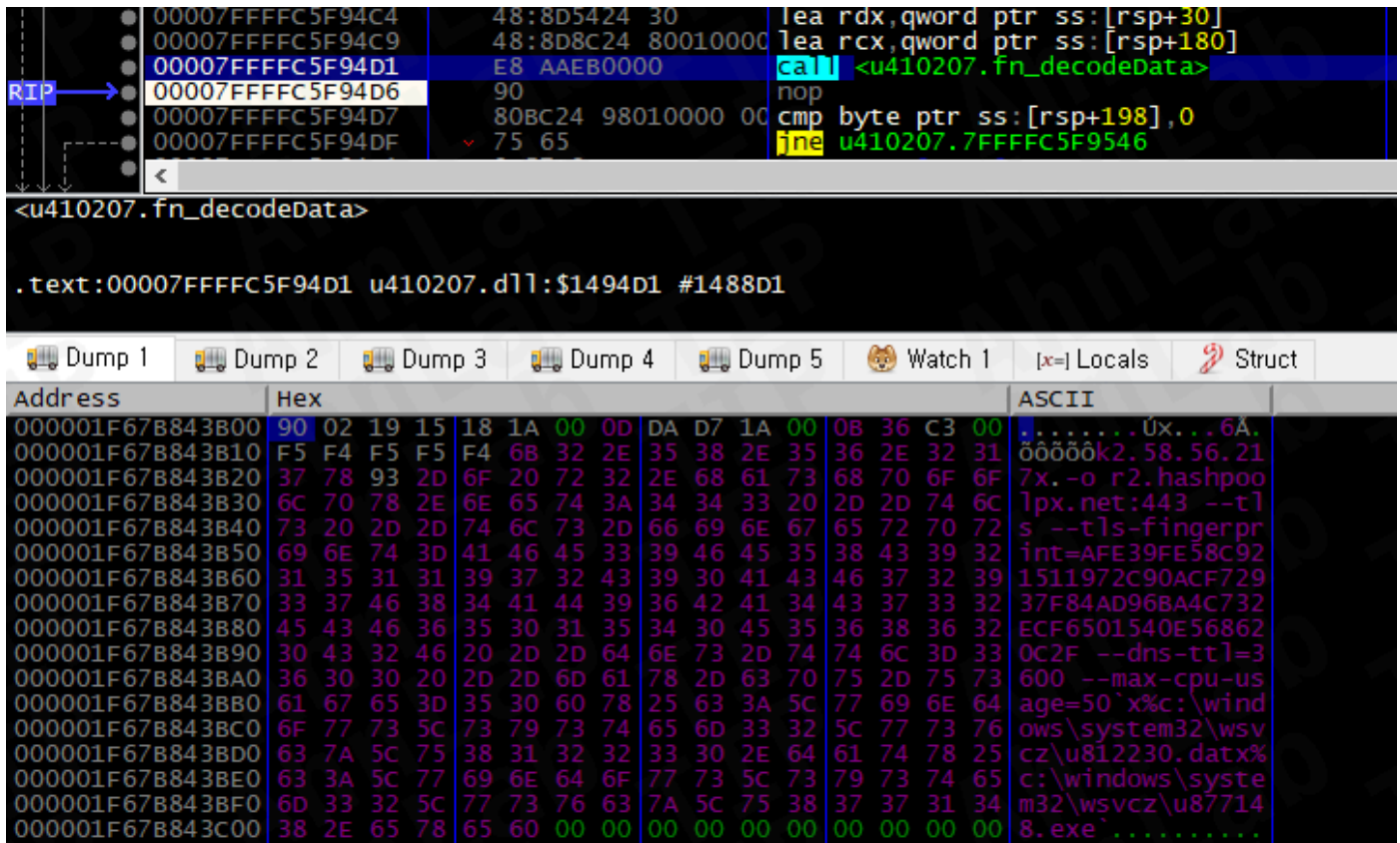


Figure 6. 업데이트된 설정 데이터

이후 USB를 담당하는 쓰레드와 및 XMRig 실행을 담당하는 쓰레드를 생성한다. USB를 담당하는 쓰레드는 위에서 다룬 바와 같이 “USB Drive.lnk” 바로 가기 파일을 생성하고 “sysvolume” 폴더에 USB 전파 악성코드 및 VBS, BAT 악성코드를 생성하며 “USB Drive” 폴더에 사용자의 파일들을 옮기는 기능을 수행한다.

XMRig 실행을 담당하는 쓰레드는 현재 실행 중인 프로세스들을 검사한 후 특정 프로세스들이 실행 중이지 않을 때에만 XMRig를 실행하고 실행 중인 경우에는 종료한다. 검사 대상 프로세스들 중에는 프로세스 검사 도구인 Process Explorer, TaskMgr, System Informer, Process Hacker 등이 있는데 이는 사용자가 현재 실행 중인 프로세스를 검사할 때 XMRig 실행 여부를 은폐하기 위한 것으로 보인다. 이외에도 많은 수의 게임 클라이언트 프로세스들이 포함되는데 이는 성능을 필요로 하는 게임 실행 중에 코인 마이너가 함께 실행된다면 성능 문제로 사용자에게 인지될 수 있기 때문인 것으로 보인다.

```
// "Taskmgr.exe"  
// "SystemInformer.exe"  
// "Processhacker.exe"  
// "procexp64.exe"  
// "procexp.exe"  
// "Adobe Premiere Pro.exe"  
// "AfterFX.exe"  
// "vegas190.exe"  
// "vegas200.exe"  
// "aces.exe"  
// "ACMirage.exe"  
// "ACOdyssey.exe"  
// "ACOrigins.exe"  
// "ACS.exe"  
// "RustClient.exe"  
// "s1_sp64_ship.exe"  
// "s2_mp64_ship.exe"  
// "s2_sp64_ship.exe"  
// "SanAndreas.exe"  
// "SCUM.exe"  
// "sdhdship.exe"  
// "sekiro.exe"  
// "ShadowOfWar.exe"  
// "ShippingPC-BmGame.exe"
```

```
// "Shivers-Win64-Shipping.exe"
// "ShooterGame.exe"
// "Bodycam.exe"
// "Sifu.exe"
// "Sifu-Win64-Shipping.exe"
// "SkaterXL.exe"
// "sniper5_dx12.exe"
// "sniperelite5.exe"
```

Figure 7. 검사 대상 프로세스 일부

XMRig 실행 인자 : “-o r2.hashpoolpx[.]net:443 -tls -tls-fingerprint=AFE39FE58C921511972C90ACF72937F84AD96BA4C732ECF6501540E568620C2F -dns-ttl=3600 -max-cpu-usage=50”



Figure 8. 프로세스 트리

5. 결론

USB는 현재까지도 악성코드를 전파하는데 악용되고 있는데 과거 오토런(autorun.inf) 기능을 악용하던 것과 달리 최근에는 사용자의 실행을 유도하는 방식이 사용되고 있다. 위의 사례를 보면 악성코드는 숨김 폴더에 존재하고 “USB Drive”라는 이름의 바로 가기 파일만 보일 수 있다. 사용자가 바로 가기 파일을 실행할 경우 악성코드뿐만 아니라 기존 사용자의 파일들을 함께 보여주기 때문에 사용자들은 악성코드가 감염되었는지 인지하는데 어려움이 있다.

공격자는 AntiVirus를 우회하는 여러 기법들을 사용해 모네로 코인을 채굴하는 XMRig를 설치하였다. XMRig는 사용자가 게임을 플레이 중이라면 종료되는 등 의심을 사지 않도록 설정되어 있으며 프로세스 검사 도구도 함께 검사하여 일반적인 도구로는 XMRig가 실행 중인 것을 확인하는데 어려움이 있다.

사용자들은 운영체제 및 설치된 소프트웨어의 최신 보안 패치를 적용해야 하며 V3 제품을 최신 버전으로 유지하여 알려진 공격을 차단해야 한다.

[V3 진단]

- Trojan/Win.SelfDel.R734002 (2025.11.08.01)
- Trojan/Win.Evo-gen.R731187 (2025.10.20.00)
- CoinMiner/Win.Agent.R735221 (2025.11.13.00)
- CoinMiner/Win.Agent.R5805841 (2025.10.18.00)
- Trojan/Win.Miner3.R512976 (2022.08.31.01)
- Trojan/BAT.RUNNER.S3110 (2025.11.27.03)
- Trojan/VBS.RUNNER.S3111 (2025.11.27.03)

MD5

1cf4a8bfd59d5f04be313d2fa3af5f5a

248eed41f083c5de46a15c2b9f30303e

4bf6fe55240267398bef02703f1a6182

916eac9c0e83da08819d49be32afa182

b88b2c61844a49fcc54727105ae9abac

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//2[.]58[.]56[.]13/inf[.]dat

http[:]//2[.]58[.]56[.]13/utl/xmr[.]dat

http[:]//2[.]58[.]56[.]13/utl/xmrsys[.]dat

FQDN

r2[.]hashpoolpx[.]net

umnsrx[.]net

IP

2[.]58[.]56[.]13

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

