

TrollAgent That Infects Systems Upon Security Program Installation Process (Kimsuky Group) - ASEC

By ATCP

Published: 2024-02-15 · Archived: 2026-04-05 18:49:03 UTC



AhnLab SEcurity intelligence Center (ASEC) recently discovered that malware strains are downloaded into systems when users try to download security programs from a Korean construction-related association’s website. Login is required to use the website’s services, and various security programs must be installed to log in. Among the programs that must be installed for login, one of the installers had malware strains inside. When the user downloads and installs the installer, the malware strains are also installed along with the security program. The two types of malware strains installed through this process are as follows: a backdoor malware that receives the threat actor’s commands externally and then carry them out, and an Infostealer that collects information from the infected systems. Therefore, users may be victims of user credentials theft, simply by installing security programs from the official website. **1. Distribution Method** Upon accessing and attempting to log in to the organization’s website, the website prompts the users to install security programs first (see Figure 1 below). Among the necessary security programs, “NX_PRNMAN” downloads the installer that has the aforementioned malware strains. This particular method is based on the time of analysis in mid-January 2024. Previously around December 2023, the malware strains were included in the security program ‘TrustPKI’ and distributed through that program. According to internal test results, the modified installer is uploaded onto the website only at specific time frames,

and only those who download the file during at this specific time frame are exposed to the attacks. Judging by the number of modified installers that AhnLab has collected, there have been over 3,000 cases of infection.

프로그램명	기능	설치상태
통합설치 프로그램 (VeraPort)	최소한 대제기술이 적용된 보안프로그램을 한번에 설치하기 위한 프로그램입니다.	미설치 다운로드
TrustPKI (TrustPKI)	공인인증서 로그인과 신고내용에 대한 전자서명을 위한 프로그램입니다.	다운로드
NX_PRNMAN (NX_PRNMAN)	출력된 전자문서의 신뢰성을 보장하기 위하여, 복사방지 마크와 고밀도 바코드를 적용한 프로그램입니다.	다운로드
UbiReport (UbiReport)	중앙서 생성/출력을 위한 프로그램입니다.	다운로드
키보드 보안 (Protect Online Security)	키보드를 통해 입력되는 정보가 유출되거나 변조되지 않도록 보호해 주는 프로그램입니다.	다운로드

Figure 1. The login process of a certain Korean website The installer is packed by VMProtect and is signed as a valid certificate from “D2Innovation”, a Korean defense company (see Figure 2). It appears that the threat actor stole a valid certificate to bypass the anti-malware product’s detection during the web browser’s download stage or file execution stage.

Figure 2. The signature information of the installer that includes malware strains The malicious installer not only installs malware but also the actual legitimate security program. The malware strains are run in the background, making it difficult for users to realize that their systems have been infected. Once the “NX_PRNMAN” installer is run, the malware strains are installed along with legitimate files in the %APPDATA% directory and are executed by the rundll32.exe process (see Figure 3).

Process	Image Path	Command
NX_PRNMAN.exe (6580)	C:\Users\... \Downloads\NX_PRNMAN.exe	"C:\Users\... \Downloads\NX_PRNMAN.exe"
cmd.exe (6206)	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe /c C:\Users\... \AppData\Local\Temp\W2E3E.tmp.bat
Conhost.exe (3906)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
rundll32.exe (1652)	C:\Windows\System32\rundll32.exe	C:\Windows\System32\rundll32.exe "C:\Users\... \AppData\Roaming\Menu\Wmenu,75018742.package" jaychoi
schtasks.exe (1492)	C:\Windows\System32\schtasks.exe	schtasks /delete /f /tn "ChromeUpdateTaskMachineUAC"
Conhost.exe (6180)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
NX_PRNMAN.tmp (3176)	C:\Users\... \Downloads\NX_PRNMAN.tmp	C:\Users\... \Downloads\NX_PRNMAN.tmp /SLS="\$1004D4,978561,57856,C:\Users\...
taskkill.exe (6992)	C:\Windows\System32\Taskkill.exe	"taskkill.exe" /f /im "UpdateManager.exe"
Conhost.exe (5036)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
cmd.exe (2356)	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe /c regsvr32 /u /s "C:\Program Files (x86)\EPS\WLB\WPRNMAN\VerMan.dll"
Conhost.exe (6436)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
regsvr32.exe (2932)	C:\Windows\System32\regsvr32.exe	regsvr32 /u /s "C:\Program Files (x86)\EPS\WLB\WPRNMAN\VerMan.dll"

Figure 3. The process tree of the malicious NX_PRNMAN installer Note that the “NX_PRNMAN” installer changed into malware in January 2024. Previously at around December 2023, the “TrustPKI” installer was used to install the same malware strains. Both malicious installers were signed with the same certificate from “D2Innovation”.

Process	Image Path	Command
NXTPKIENT.exe (660)	C:\Users\... \Downloads\NXTPKIENT.exe	"C:\Users\... \Downloads\NXTPKIENT.exe"
cmd.exe (1192)	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe /c C:\Users\... \AppData\Local\Temp\WASA1.tmp.bat
Conhost.exe (612)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
rundll32.exe (1132)	C:\Windows\System32\rundll32.exe	C:\Windows\System32\rundll32.exe "C:\Users\... \AppData\Roaming\Media\Wwir-12954a3.db" kimyy
schtasks.exe (4796)	C:\Windows\System32\schtasks.exe	schtasks /delete /f /tn "ChromeUpdateTaskMachineUAC"
Conhost.exe (4992)	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1
NXTPKIENTS.exe (4600)	C:\Users\... \Downloads\NXTPKIENTS.exe	"C:\Users\... \Downloads\NXTPKIENTS.exe"
NXTPKIENTS.tmp (4664)	C:\Users\... \AppData\Local\Temp\Wis-R8...	"C:\Users\... \AppData\Local\Temp\Wis-R8KF.tmp\NXTPKIENTS.tmp" /SLS="\$902B8,6291726,231424,C...
NXTPKIENTS.exe (5)	C:\Users\... \Downloads\NXTPKIENTS.exe	"C:\Users\... \Downloads\NXTPKIENTS.exe" /SPA\W\ND=\$2047C /NOTIF\Y\ND=\$902B8
NXTPKIENTS.tmp	C:\Users\... \AppData\Local\Temp\Wis-9L...	"C:\Users\... \AppData\Local\Temp\Wis-9LROB.tmp\NXTPKIENTS.tmp" /SLS="\$4044C,6291726,231424,C...
taskkill.exe (1)	C:\Windows\System32\Taskkill.exe	"C:\Windows\System32\Taskkill.exe" /f /im iexplore.exe
Conhost.exe	C:\Windows\System32\Conhost.exe	W??WC:\Windows\System32\Conhost.exe 0xffffffff -ForceV1

Figure 4. The malicious TrustPKI installer’s process tree “TrustPKI” is the first discovered malware that was signed with the valid certificate of “D2Innovation”. It was a disguised malware created on December 12th, 2023, and the latest disguised malware is the “NX_PRNMAN” developed on January 11th, 2024.

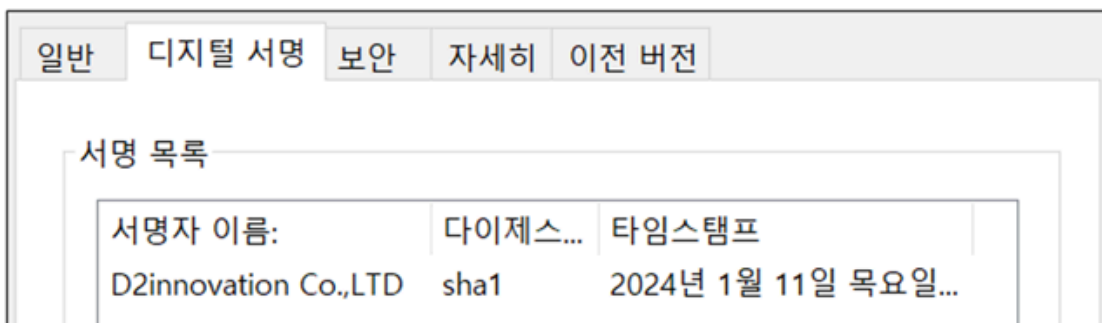
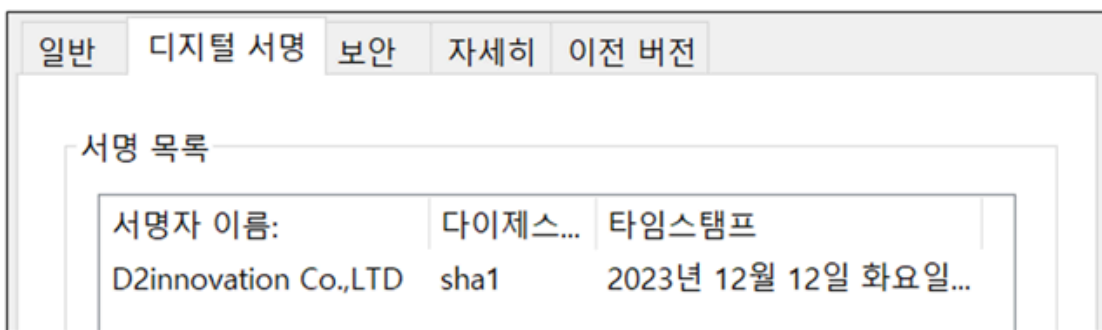


Figure 5. Signature information discovered since 2023 **2. Analysis of Installed Malware 2.1. Infostealer (TrollAgent)** The malicious installer and most of the malware strains that are actually installed are packed by VMProtect and developed in GoLang. Most notably, malware created in the %APPDATA% directory by malicious installers is Infostealer, which is malware that steals data from infected systems. It is developed in GoLang and is executed through rundll32.exe due to its DLL format. With the source code information (written in GoLang) inside in the binary, malware named “troll” created by the threat actor was discovered. The TrollAgent Infostealer provides multiple features that not only steal system information, but also credentials, cookies, bookmarks, history, and extensions saved in web browsers such as Chrome and Firefox.

```
String
D:/~/repo/golang/src/root.go/s/troll/agent/cmd/cmd.go
D:/~/repo/golang/src/root.go/s/troll/agent/config/config.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/bookmark/bookmark.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/browsingdata.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/cookie/cookie.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/creditcard/creditcard.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/download/download.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/extension/extension.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/history/history.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/localstorage/localstorage.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/outputter.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browsingdata/password/password.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browser/browser.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browser/browser_windows.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browser/chromium/chromium.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browser/chromium/chromium_windows.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browser/firefox/firefox.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/decrypter/decrypter.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/decrypter/decrypter_windows.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/item/item.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/utils/fileutil/fileutil.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/utils/typeutil/typeutil.go
D:/~/repo/golang/src/root.go/s/troll/agent/main/main.go
D:/~/repo/golang/src/root.go/s/troll/agent/msg/msg.go
D:/~/repo/golang/src/root.go/s/troll/agent/neti/neti.go
D:/~/repo/golang/src/root.go/s/troll/agent/npwww/npwww.go
```

Figure 6. Troll Infostealer’s source code **2.2. Backdoor (GoLang / C++)** Most of the malicious installers install the Troll Infostealer, but may also simultaneously install backdoor malware strains. The C&C branching commands of the backdoor malware strains used in these attacks are similar to the ones introduced in the following articles: “**AppleSeed Being Distributed to Nuclear Power Plant-Related Companies**” [\[1\]](#) uploaded in November 2022, and “**Kimsuky Targets South Korean Research Institutes with Fake Import Declaration**” [\[2\]](#) uploaded in November 2023.

Dropper/Win.TrollAgent.C5572219 (2024.01.12.02) – Dropper/Win.TrollAgent.C5572604 (2024.01.12.02) –
Dropper/Win.TrollAgent.C5572605 (2024.01.12.02) – Dropper/Win.TrollAgent.C5572607 (2024.01.12.02) –
Dropper/Win.TrollAgent.C5572629(2024.01.12.02) – Infostealer/Win.TrollAgent.C5572217 (2024.01.12.02) –
Infostealer/Win.TrollAgent.C5572601 (2024.01.12.02) – Infostealer/Win.TrollAgent.R630772 (2024.01.12.02) –
Backdoor/Win.D2Inv.C5572602 (2024.01.12.02) – Backdoor/Win.D2Inv.C5572603 (2024.01.12.02)

MD5

013c4ee2b32511b11ee9540bb0fdb9d1

035cf750c67de0ab2e6228409ac85ea3

19c2decfa7271fa30e48d4750c1d18c1

27ef6917fe32685fdf9b755eb8e97565

2aaa3f1859102aab35519f0d4c1585dd

Additional IOCs are available on AhnLab TIP.

URL

http[:]//ai[.]aerosp[.]p-e[.]kr/index[.]php

http[:]//ai[.]bananat[.]p-e[.]kr/index[.]php

http[:]//ai[.]daysol[.]p-e[.]kr/index[.]php

http[:]//ai[.]kimyy[.]p-e[.]kr/index[.]php

http[:]//ai[.]kostin[.]p-e[.]kr/index[.]php

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.



Source: <https://asec.ahnlab.com/en/61934/>