asec.ahnlab.com /en/61934/

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

By ASEC ⋮⋮ 2/23/2024

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.

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.

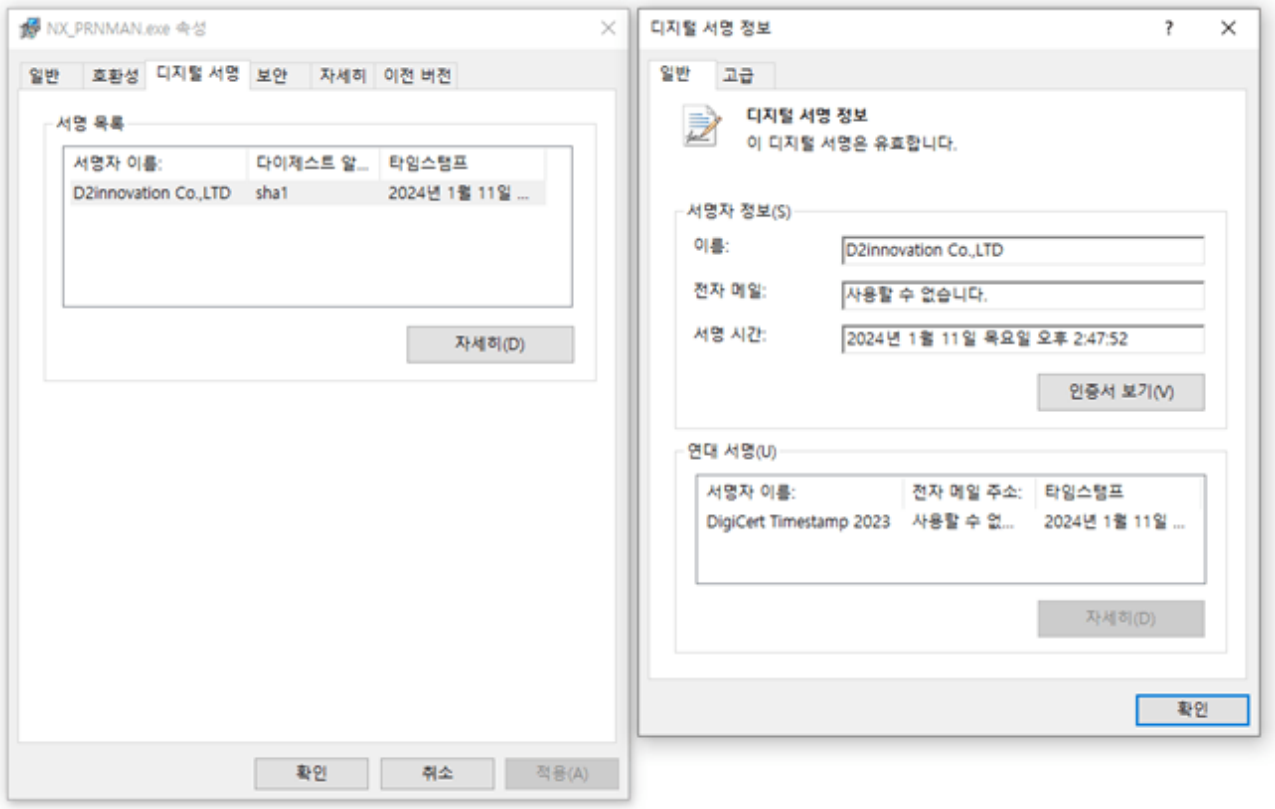

Figure 2. The signature information of the installer that includes malware strains

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).

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 “D2Innvation”.

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.

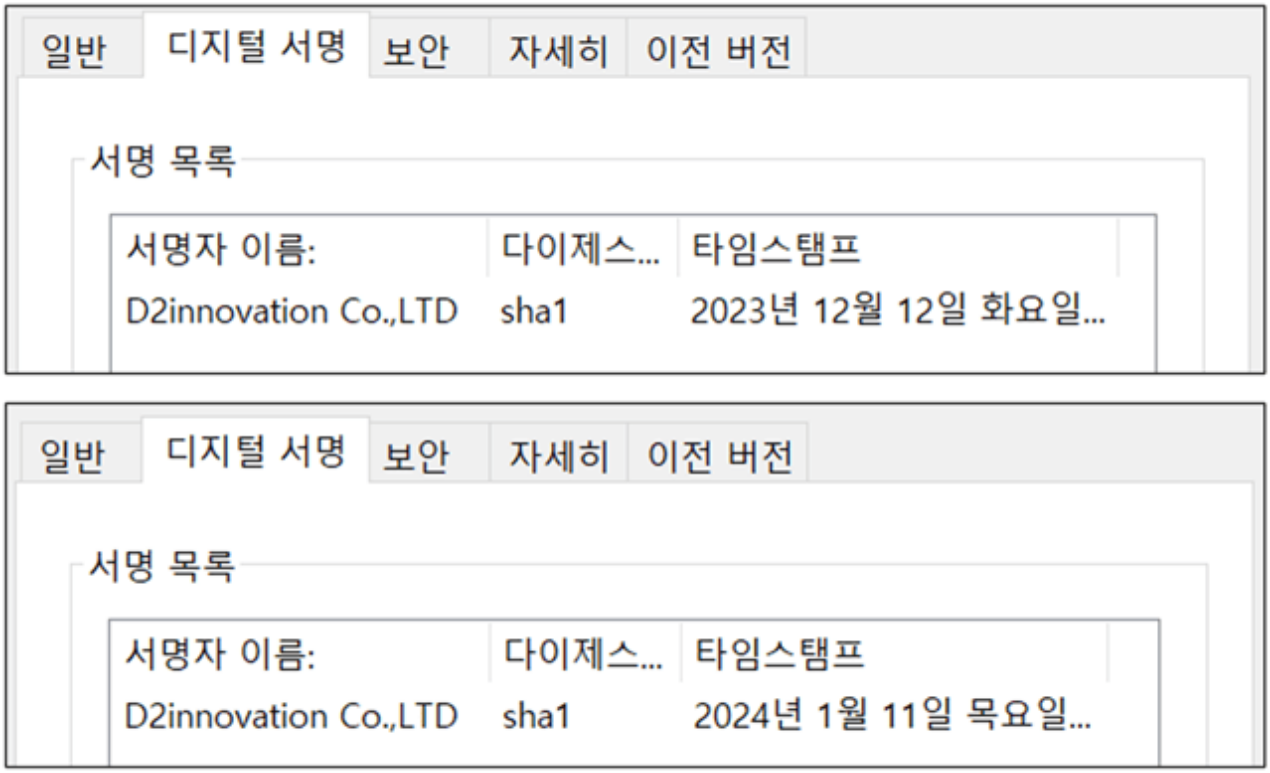

Figure 5. Signature information discovered since 2023

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/browingdata/bookmark/bookmark.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/browsingdata.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/cookie/cookie.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/creditcard/creditcard.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/download/download.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/extension/extension.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/history/history.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/localstorage/localstorage.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/outputter.go
D:/~/repo/golang/src/root.go/s/troll/agent/internal/browingdata/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/filetutil.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/npww/npww.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.

```
wcscpy(v16, L"sdel ");
if ( wcsnicmp((const wchar_t *)hMem, v16, 5ui64) )
{
  wcscpy((wchar_t *)v27, L"getinfo");
  if ( wcsnicmp((const wchar_t *)hMem, (const wchar_t *)v27, 7ui64) )
  {
    wcscpy(v23, L"scr");
    if ( wcsnicmp((const wchar_t *)hMem, v23, 3ui64) )
    {
      wcscpy(v24, L"up ");
      if ( wcsnicmp((const wchar_t *)hMem, v24, 3ui64) )
      {
        wcscpy(v25, L"dn ");
        if ( wcsnicmp((const wchar_t *)hMem, v25, 3ui64) )
        {
          wcscpy(v26, L"die");
          if ( !wcsnicmp((const wchar_t *)hMem, v26, 3ui64) )
            goto LABEL_27;
```

Figure 7. Branching commands of the backdoor malware strains (C++)

For this attack, the threat actor also utilized backdoor malware strains developed in GoLang with a similar form to the previous backdoor malware strains.

```
mirror/En/En/Kernel.Process_Download.func1
mirror/En/En/Kernel.Process_Exit
mirror/En/En/Kernel.Process_GetInfo
mirror/En/En/Kernel.Process_GetInfo.func1
mirror/En/En/Kernel.Process_Hibernate
mirror/En/En/Kernel.Process_Pwd
mirror/En/En/Kernel.Process_Sleep
mirror/En/En/Kernel.Process_SocksAdd
mirror/En/En/Kernel.Process_SocksAdd.func1
mirror/En/En/Kernel.Process_SocksList
mirror/En/En/Kernel.Process_Unknown
mirror/En/En/Kernel.Process_Upload
mirror/En/En/Kernel.Process_Where
mirror/En/En/Kernel.RunShell
mirror/En/En/Kernel.RunShell.func1
mirror/En/En/Kernel.SelfDeleteExit
mirror/En/En/Kernel.SelfDeleteExit.func1
mirror/En/En/Kernel.SelfDeleteExit.func2
mirror/En/En/Kernel.SelfDeleteExit.func3
mirror/En/En/Kernel.SelfDeleteExit.func4
mirror/En/En/Kernel.SetConnTime
mirror/En/En/Kernel.SetConnTime.func1
mirror/En/En/Kernel.StartClient
mirror/En/En/Kernel.UploadResult
mirror/En/En/Kernel.UploadResult.func1
mirror/En/En/Kernel/en.go
mirror/En/En/Kernel/revsocks.go
mirror/En/En/Kernel/shell_windows.go
mirror/En/En/exe/main.go
```

Figure 8. Backdoor malware strains developed in GoLang

3. Conclusion

Recently, malware disguised as a legitimate security program was uploaded to a Korean construction-related association's website. When users install security programs to log into the website, malware strains may also be installed along with the legitimate security program. The malware strains can steal user information stored in infected systems and receive commands from the threat actor via the C&C server to perform various malicious activities.

Users must update V3 to the latest version so that malware infection can be prevented.

File Detection

– 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)

IOC

MD5

– 9e75705b4930f50502bcbd740fc3ece1: Malicious installer (TrustPKI)
– 27ef6917fe32685fdf9b755eb8e97565: Malicious installer (TrustPKI)
– 62fba369711087ea37ef0b0ab62f3372: Malicious installer (TrustPKI)
– e4a6d47e9e60e4c858c1314d263aa317: Malicious installer (TrustPKI)
– 6097d030fe6f05ec0249e4d87b6be4a6: Malicious installer (TrustPKI)
– b532f3dcc788896c4844f36eb6cee3d1: Malicious installer (TrustPKI)
– b97abf7b17aeb4fa661594a4a1e5c77f: Malicious installer (TrustPKI)
– d67abe980a397a94e1715df6e64eedc8: Malicious installer (TrustPKI)
– 2aaa3f1859102aab35519f0d4c1585dd: Malicious installer (TrustPKI)
– 7b6d02a459fdaa4caa1a5bf741c4bd42: Malicious installer (TrustPKI)
– 19c2decfa7271fa30e48d4750c1d18c1: Malicious installer (NX_PRNMAN)
– 4168ff8b0a3e2f7e9c96afb653d42a01: Malicious installer (NX_PRNMAN)
– a67cf9add2905c11f5c466bc01d554b0: TrollAgent Infostealer
– 7457dc037c4a5f3713d9243a0dfb1a2c: TrollAgent Infostealer
– 42ea65fda0f92bbeca5f4535155125c7: TrollAgent Infostealer
– 4222492e069ac78a55d3451f4b9b9fca: TrollAgent Infostealer
– dc636da03e807258d2a10825780b4639: TrollAgent Infostealer
– 9360a895837177d8a23b2e3f79508059: TrollAgent Infostealer
– 035cf750c67de0ab2e6228409ac85ea3: TrollAgent Infostealer
– 013c4ee2b32511b11ee9540bb0fdb9d1: TrollAgent Infostealer
– 88f183304b99c897aacfa321d58e1840: TrollAgent Infostealer
– c8e7b0d3b6afa22e801cacaf16b37355: TrollAgent Infostealer
– 2b678c0f59924ca90a753daa881e9fd3: TrollAgent Infostealer
– 8d4af59eebdcda10f3c88049bb097a3a: Backdoor (C++)
– 87429e9223d45e0359cd1c41c0301836: Backdoor (GoLang)

C&C

– hxxp://sa.netup.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://dl.netup.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.kimyy.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ve.kimyy.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ar.kostin.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.kostin.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://pe.daysol.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.daysol.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ca.bananat.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.bananat.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://pi.selecto.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.selecto.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.aerosp.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ce.aerosp.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.limsjo.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://qi.limsjo.p-e[.]kr/index.php: TrollAgent Infostealer

– hxxp://ai.ssungmin.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://li.ssungmin.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ai.negapa.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://ol.negapa.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://qa.jaychoi.p-e[.]kr/index.php: TrollAgent Infostealer
– hxxp://viewer.appofficer.kro[.]kr/index.php: Backdoor (C++)
– hxxp://coolsystem.co[.]kr/admin/mail/index.php: Backdoor (GoLang)

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Kimsuky,Security Program,TrollAgent