Posted on March 23, 2022

Word Document Attack Targeting Companies Specialized in Carbon Emissions

On March 18th, the ASEC analysis team discovered a document-borne APT attack targeting companies specialized in carbon emissions. According to logs collected from AhnLab's ASD (AhnLab Smart Defense), the user of the infected PC appears to have downloaded a malicious word document titled "**** Carbon Credit Institution.doc" through a web browser.

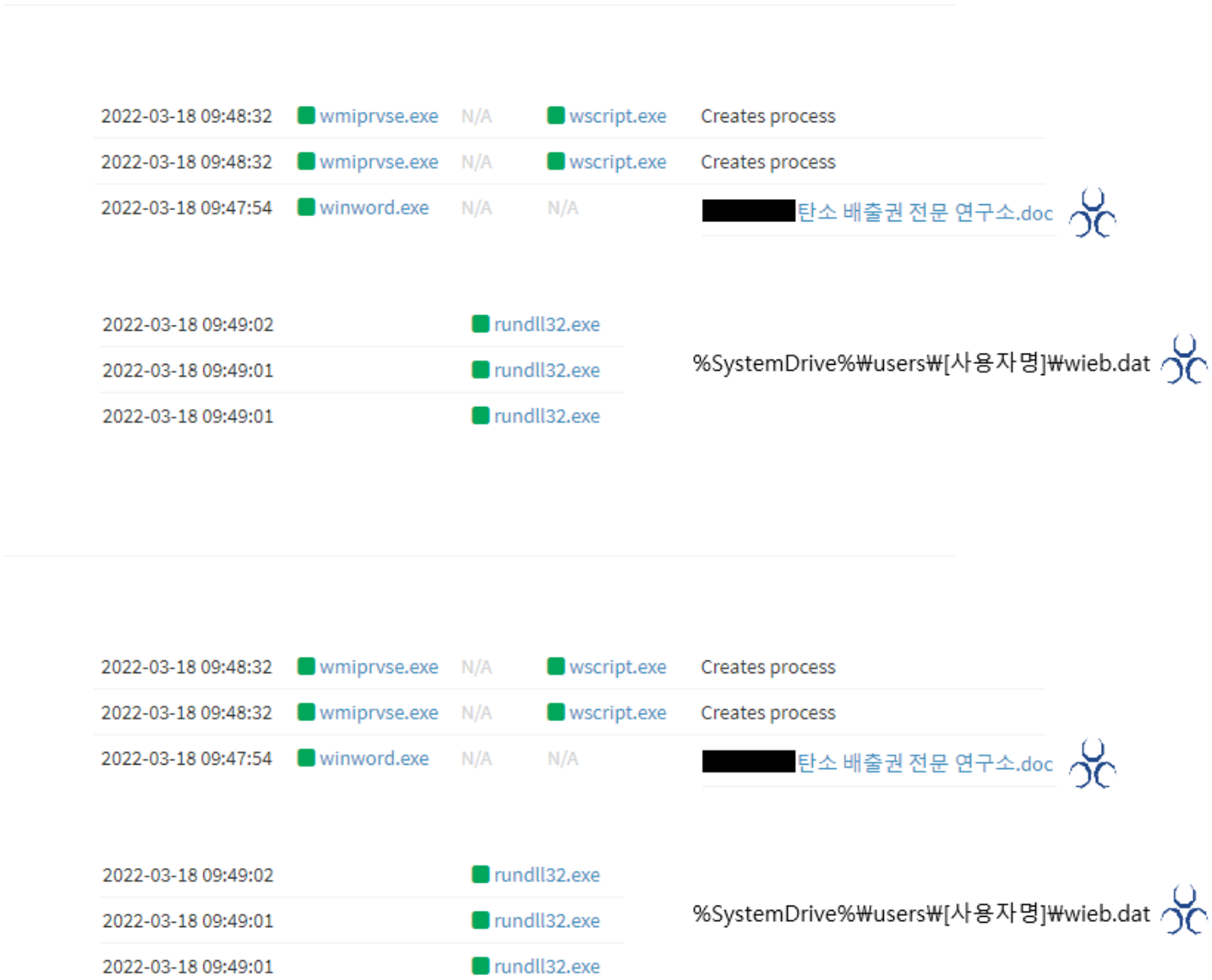

Figure 1. Logs secured by ASD infrastructure

While the malicious document could not be secured, it is likely that its internal macro code runs wscript.ex. The confirmed execution argument for wscript.exe is as follows:

- wscript.exe %AppData%\Microsoft\Templates\version.ini

The method of using an execution argument is the same as the technique used by the same attacker group in the past. In the previous case, the malware created a task scheduler in the infected PC when version.ini consisting of VBS code was run. It then performed malicious behaviors by receiving additional payloads from the attacker's C&C server. It appears that for the current case, additional attacks took place following a similar method.

The additional attacks for the current case were done by running the Gold Dragon malware on the infected PC. The attacker seems to have created and ran the DLL that installs Gold Dragon in the %HomePath% path with the name "wieb.dat".

Gold Dragon that is run has similar features as the malware mentioned in the following ASEC blog post:

> Distribution of Kimsuky Group's xRAT (Quasar RAT) Confirmed

However, whereas the Gold Dragon in the previous case was not equipped with the module that leaks information, the current one has it built-in.

The module included the feature for running commands shown below as well as keylogging and leaking clipboard.

- cmd.exe /c ipconfig/all >>"%s" & arp -a >>"%s"
- cmd.exe /c systeminfo >>"%s"

- cmd.exe /c tasklist >>"%s"

The leaked information is saved in the path '%localappdata%\Microsoft\common\pre' as shown in Figure 2.

- FreedsStore.feedsdb-ms: Saves keylogged data
- PI_000.dat: Saves list of files within folders C:\Program Files and C:\users
- PI_001.dat: Saves system information, process list, and IP information (saving execution results of ipconfig, systeminfo, and tasklist)

Figure 2. Data files saved with the leaked information

The attacker group is performing attacks on multiple industries. As such, users should take extreme caution not to open attachments of posts and emails with unknown sources.

AhnLab products are consistently monitoring and responding to APT attacks mentioned in this post. For Gold Dragon, they are responding under the following information.

[IOC] [MD5, alias, and engine version] wieb.dat: c096ceaaecd4c8fccfe765280a6dac1e Trojan/Win.Kimsuky.C5016729 (2022.03.19.00) Gold Dragon: dd468bb6daff412f0205b21d50ddd641 Trojan/Win.Kimsuky.C5016818 (2022.03.19.00)

[C&C] Gold Dragon download URL (wieb.dat): hxxps://osp06397.net/view.php?id=21504 Gold Dragon C&C: hxxps://us43784.org/report.php

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

Categories:Malware Information

Tagged as:APT, Gold Dragon, Kimsuky