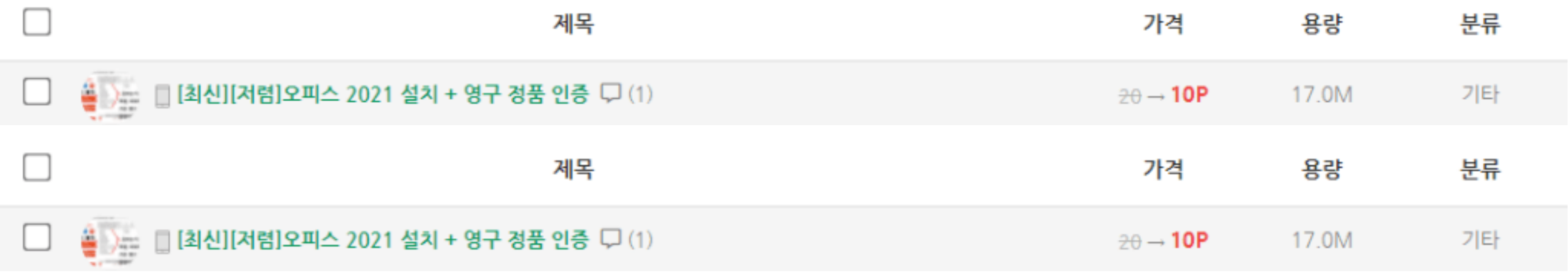
Posted on March 28, 2022

BitRAT Disguised as Officer Installer Being Distributed

The ASEC analysis team previously uploaded a post about BitRAT that was distributed under the disguise of Windows OS license verification tool. The BitRAT is now being distributed as Office Installer with different files, preying upon potential victims.

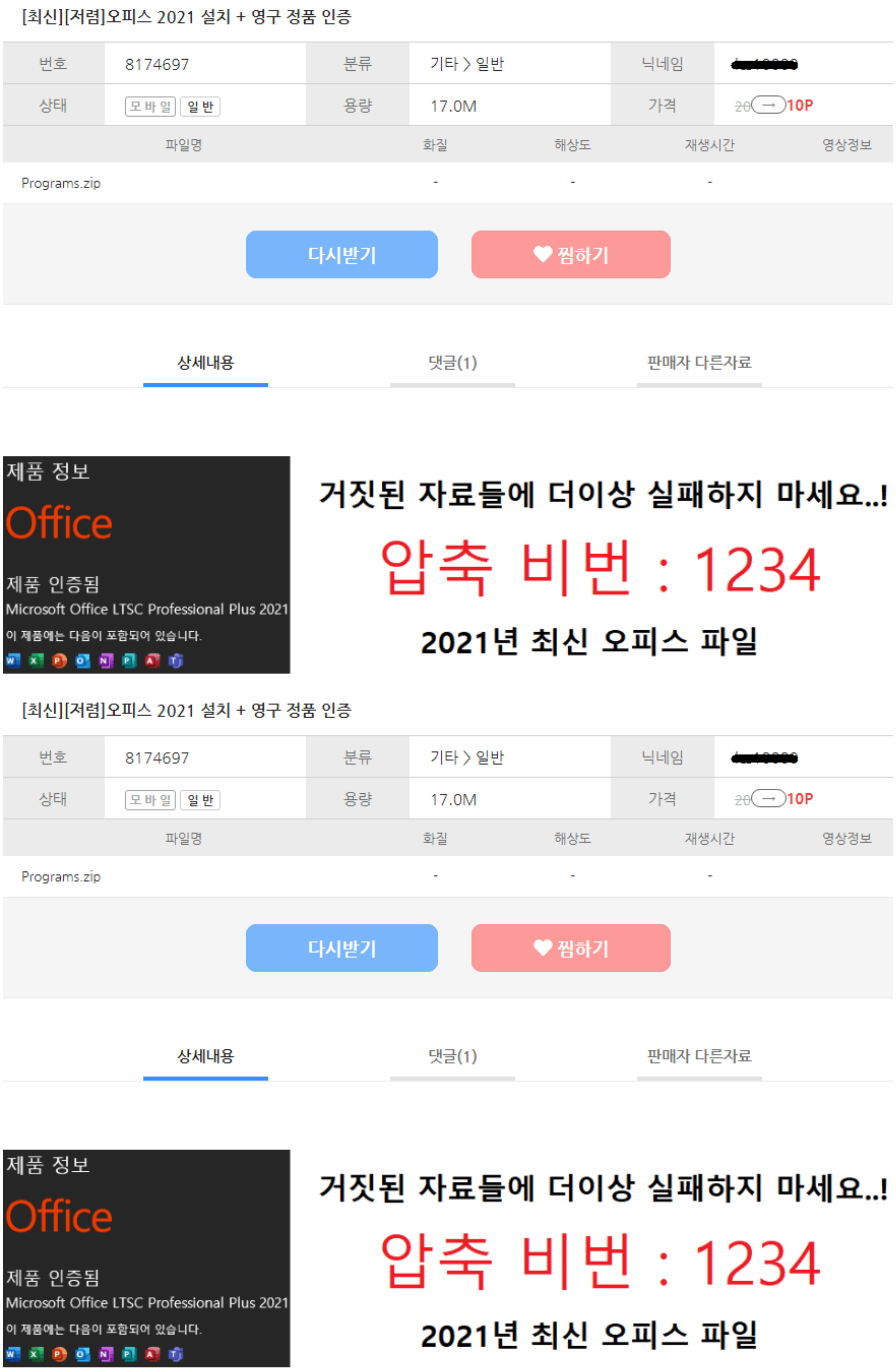
> BitRAT Disguised as Windows Product Key Verification Tool Being Distributed

The following image shows a post that contains the malware. It is titled, [New][Cheap]Office 2021 Installer + Permanent License Verification.



□	제목	가격	용량	분류
□	[최신][저렴]오피스 2021 설치 + 영구 정품 인증 (1)	~~20~~ → 10P	17.0M	기타
□	제목	가격	용량	분류
□	[최신][저렴]오피스 2021 설치 + 영구 정품 인증 (1)	~~20~~ → 10P	17.0M	기타

Figure 1. Post disguised as download of Windows license verification tool — 1



[최신][저렴]오피스 2021 설치 + 영구 정품 인증

번호	8174697	분류	기타 〉 일반	닉네임	[redacted]
상태	모 바 일 일 반	용량	17.0M	가격	~~20~~ → 10P

파일명	화질	해상도	재생시간	영상정보
Programs.zip	-	-	-	

다시받기
♥ 찜하기
상세내용
댓글(1)
판매자 다른자료
제품 정보
Office
제품 인증됨
Microsoft Office LTSC Professional Plus 2021
이 제품에는 다음이 포함되어 있습니다.

거짓된 자료들에 더이상 실패하지 마세요..!

압축 비번 : 1234

2021년 최신 오피스 파일

[최신][저렴]오피스 2021 설치 + 영구 정품 인증

번호	8174697	분류	기타 〉 일반	닉네임	[redacted]
상태	모 바 일 일 반	용량	17.0M	가격	~~20~~ → 10P

파일명	화질	해상도	재생시간	영상정보
Programs.zip	-	-	-	

거짓된 자료들에 더이상 실패하지 마세요..!

압축 비번 : 1234

2021년 최신 오피스 파일

Figure 2. Post disguised as download of Windows license verification tool — 2

The downloaded file is a compressed file named ‘Program.zip’, just like the one introduced in the previous blog post (see Figure 3 and Figure 4). As per the post description, the password of this compressed file is ‘1234’. The compressed file contains Office installer named ‘OInstall.exe’.

Figure 3. Downloaded compressed file

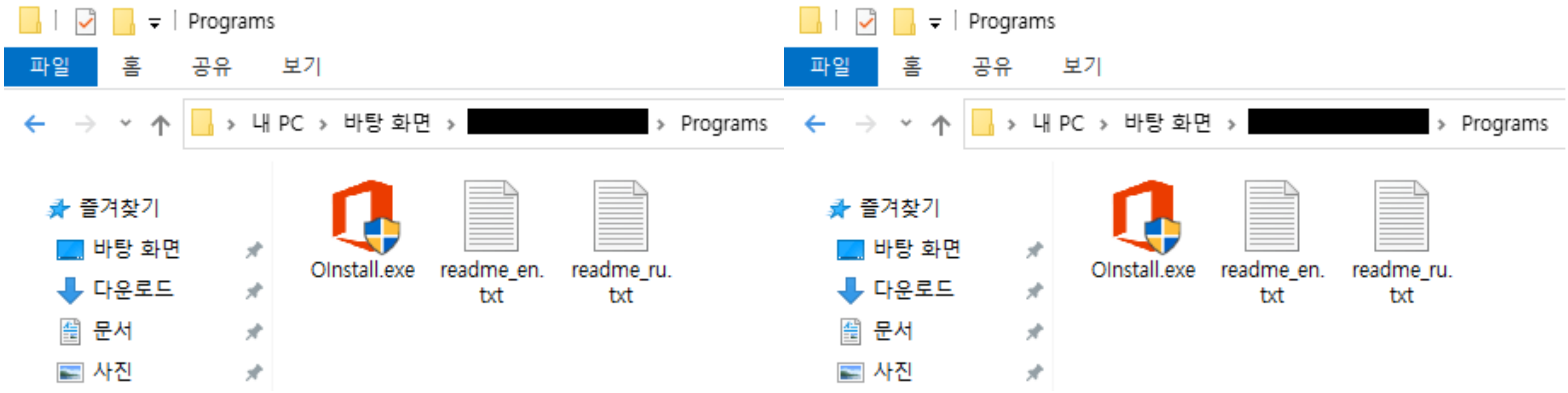
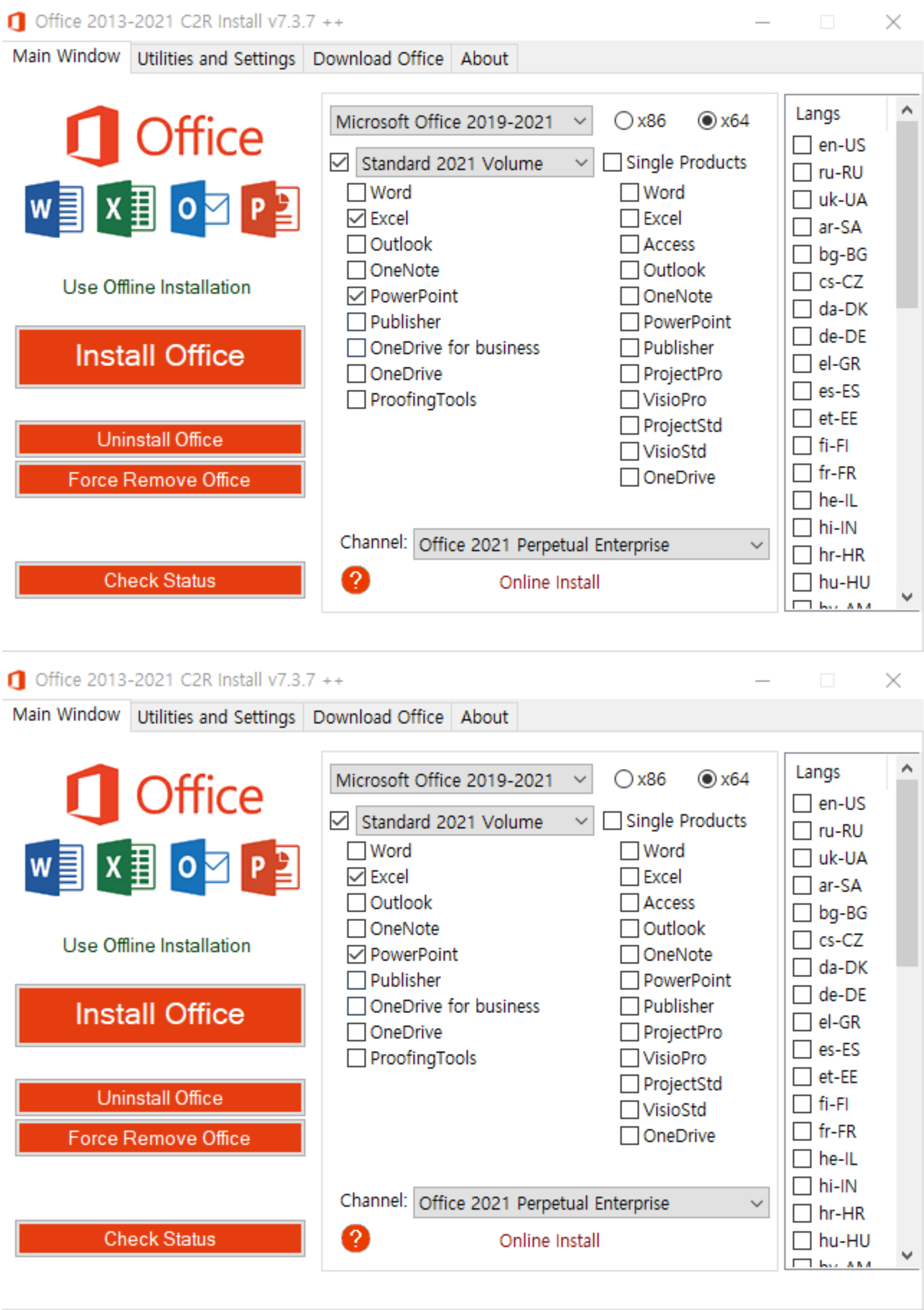


Figure 4. Files included in the compressed file

The pop-up the victim gets is that of the Office downloader (see Figure 5), but the actual downloader installs it in the startup folder (see Figure 6). Normally, the first file that is installed is a downloader of the same kind, and the downloader run this way ultimately installs BitRAT into the path %TEMP% as 'Software_Reporter_Tool.exe'.



Microsoft Office 2019-2021 ○ x86 ● x64

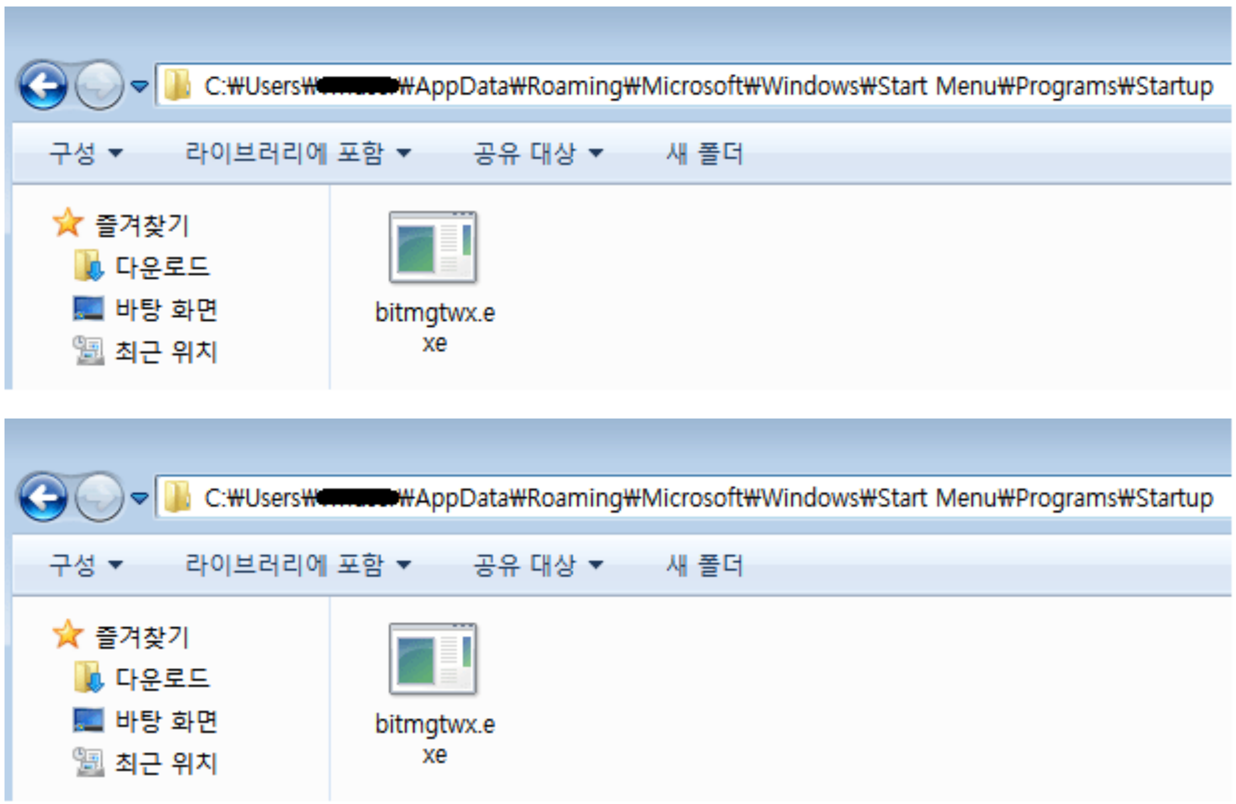
☑ Standard 2021 Volume ☐ Single Products

☐ Word ☐ Word
☑ Excel ☐ Excel
☐ Outlook ☐ Access
☐ OneNote ☐ Outlook
☑ PowerPoint ☐ OneNote
☐ Publisher ☐ PowerPoint
☐ OneDrive for business ☐ Publisher
☐ OneDrive ☐ ProjectPro
☐ ProofingTools ☐ VisioPro
☐ ProjectStd
☐ VisioStd
☐ OneDrive

Channel: Office 2021 Perpetual Enterprise

☐ en-US
☐ ru-RU
☐ uk-UA
☐ ar-SA
☐ bg-BG
☐ cs-CZ
☐ da-DK
☐ de-DE
☐ el-GR
☐ es-ES
☐ et-EE
☐ fi-FI
☐ fr-FR
☐ he-IL
☐ hi-IN
☐ hr-HR
☐ hu-HU

Figure 5. Office downloader pop-up the victims get



C:₩Users₩[redacted]₩AppData₩Roaming₩Microsoft₩Windows₩Start Menu₩Programs₩Startup

bitmgtwx.exe

Figure 6. Actual malware (BitRAT downloader) secretly downloaded

The following lists features of BitRAT.

1. Network Communication Method — Encrypted communication using TLS 1.2 — Communication using Tor

2. Basic Control — Process manager — Service manager — File manager — Windows manager — Software manager

3. Information Theft — Keylogging — Clipboard logging — Webcam logging — Audio logging — Application (e.g. Web browsers) account credential theft

4. Remote Control — Remote desktop — hVNC (Hidden Desktop)

5. Proxy — SOCKS5 Proxy: port forwarding feature using UPnP — Reverse Proxy: SOCKS4 Proxy

6. Coin Mining — XMRig CoinMiner

7. etc. — DDoS attack — UAC Bypass — Windows Defender deactivation

As shown in the examples above, the malware is being distributed actively via file-sharing websites such as Korean webhards. As such, caution is advised when running executables downloaded from a file-sharing website. It is recommended for the users to download products from the official websites of developers.

AhnLab's anti-malware software, V3, detects and blocks the malware above using the aliases below.

[File Detection] — Downloader/Win.BitRAT.C5018635 (2022.03.22.03) — Downloader/Win.BitRAT.R479001 (2022.03.22.03) — Backdoor/Win.BitRAT.C5023733 (2022.03.22.03)

[Behavior Detection] — Malware/MDP.Download.M1197

[IOC] Downloader malware MD5 8efb366f0adeeb32e66ea03eff4f50f8 56fbf1d1f2737a2d3c05b2dbc7bb0ca6 72869b470b5fe354db412283b4172a47 08634ba1bdf3d4594887a9a7a44c7ab1

BitRAT MD5 d632849a9033f24257439988533d31f2

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

Categories:Malware Information, Others