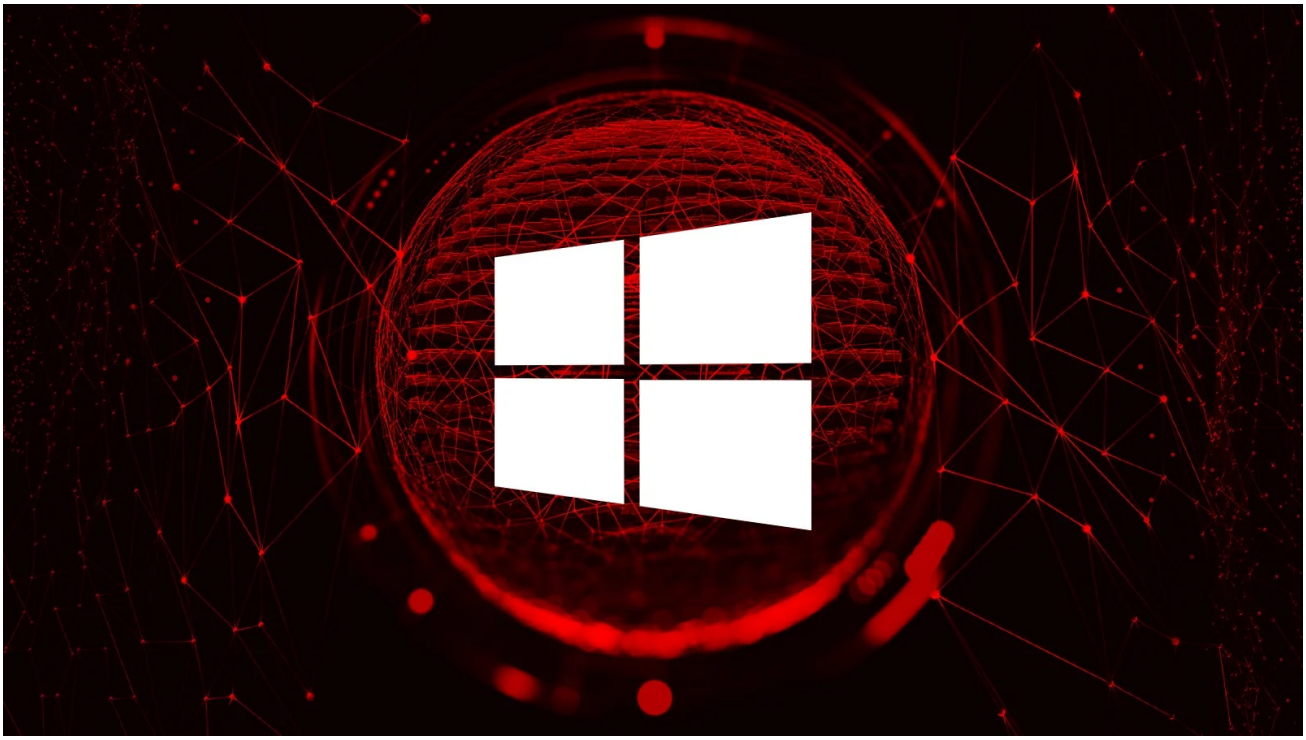
# BitRAT malware now spreading as a Windows 10 license activator

bleepingcomputer.com/news/security/bitrat-malware-now-spreading-as-a-windows-10-license-activator/

Bill Toulas

By
Bill Toulas

- March 21, 2022
- 05:18 PM
- 0



A new BitRAT malware distribution campaign is underway, exploiting users looking to activate pirated Windows OS versions for free using unofficial Microsoft license activators.

BitRAT is a powerful remote access trojan sold on cybercrime forums and dark web markets for as low as $20 (lifetime access) to any cybercriminal who wants it.

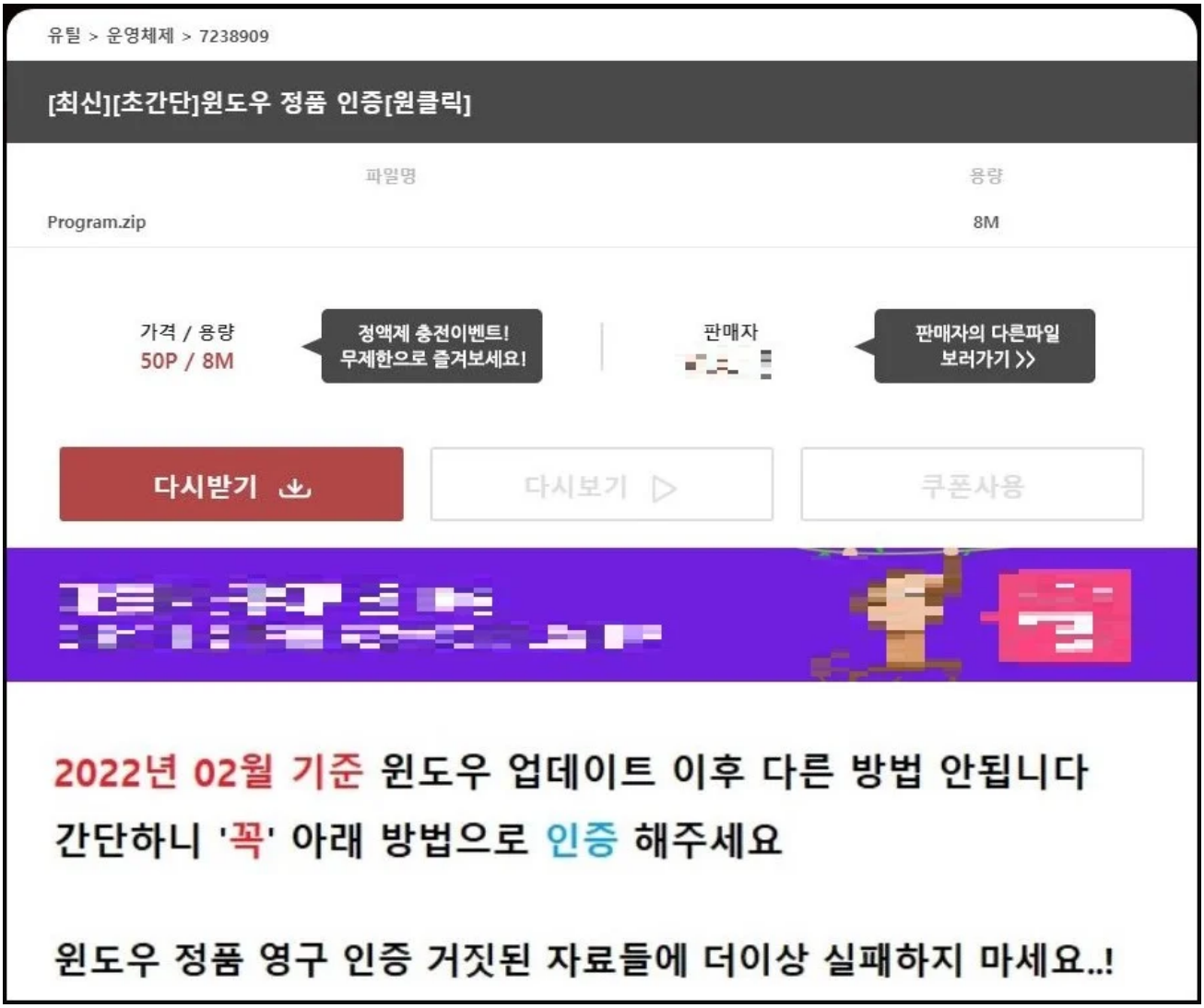
As such, each buyer follows their own approach to malware distribution, ranging from phishing, watering holes, or trojanized software.

## Targeting pirates with malware

In a new BitRAT malware distribution campaign discovered by researchers at AhnLab, threat actors are distributing the malware as a Windows 10 Pro license activator on webhards.

Webhards are online storage services popular in South Korea that have a steady influx of visitors from direct download links posted on social media platforms or Discord. Due to their wide use in the region, threat actors are now more commonly using webhards to distribute malware.

The actor behind the new BitRAT campaign appears to be Korean based on some of the Korean characters in the code snippets and the manner of its distribution.

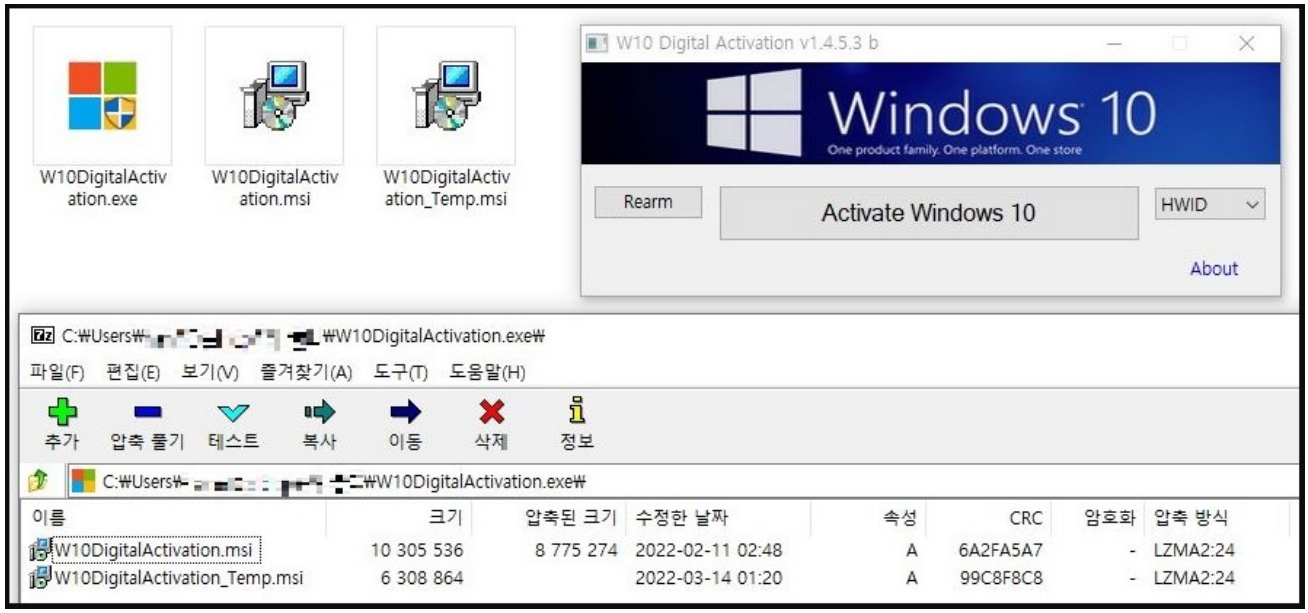



**Post promoting the BitRAT dropping Windows activator** *(ASEC)*

To properly use Windows 10, you need to purchase and activate a license with Microsoft. While there are ways to get Windows 10 for free, you still need a valid Windows 7 license to get the free upgrade.

Those who do not want to deal with licensing issues or do not have a license to upgrade commonly turn to pirating Windows 10 and using unofficial activators, many of which contain malware.

In this campaign, the malicious file promoted as a Windows 10 activator is named 'W10DigitalActiviation.exe' and features a simple GUI with a button to "Activate Windows 10."

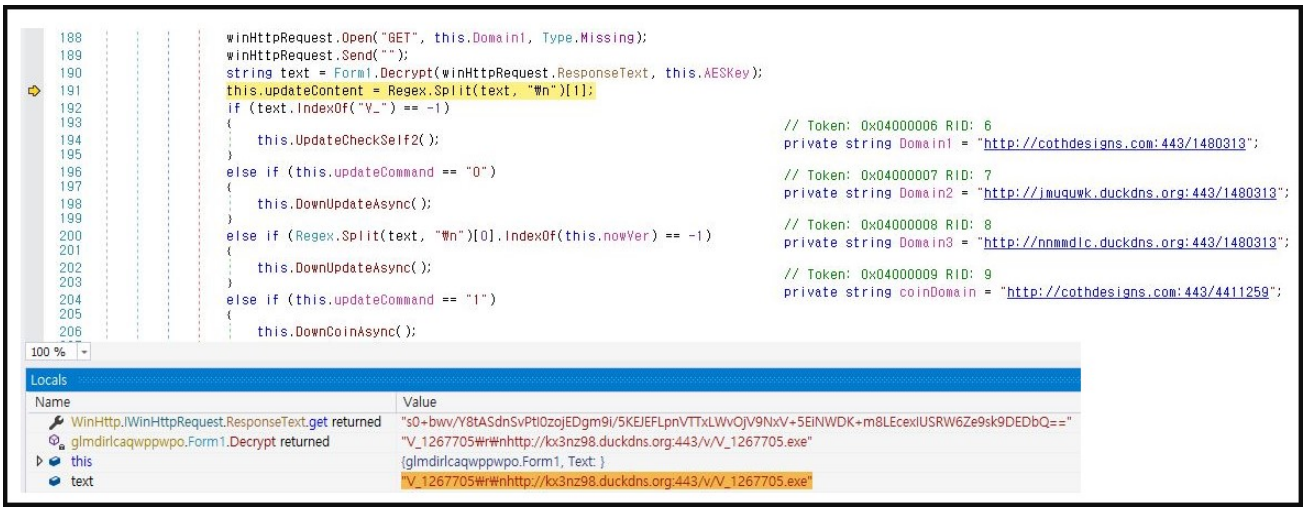



**The malware downloader posing as a Windows activator** *(ASEC)*

However, instead of activating the Windows license on the host system, the "activator" will download malware from a hardcoded command and control server operated by the threat actors.

The fetched payload is BitRAT, installed in %TEMP% as ‘Software_Reporter_Tool.exe’ and added to the Startup folder. The downloader also adds exclusions for Windows Defender to ensure that BitRAT won’t encounter detection issues.

Once the malware installation process is completed, the downloader deletes itself from the system leaving behind only BitRAT.




**The downloader fetching the BitRAT payload** *(ASEC)*

## A versatile RAT

BitRAT is promoted as a powerful, inexpensive, and versatile malware that can snatch a wide range of valuable information from the host, perform DDoS attacks, UAC bypass, etc.

BitRAT supports generic keylogging, clipboard monitoring, webcam access, audio recording, credential theft from web browsers, and XMRig coin mining functionality.

Additionally, it offers remote control for Windows systems, hidden virtual network computing (hVNC), and reverse proxy through SOCKS4 and SOCKS5 (UDP). On that front, ASEC's analysts have found strong code similarities with TinyNuke, and its derivative, AveMaria (Warzone).

The hidden desktop feature on these RATs is so valuable that some hacking groups, like the Kimsuky, incorporated them in their arsenal just to use the hVNC tool.

## Risk of piracy

Even if the legal and ethical aspects are ignored, using pirated software is always a security gamble.

The more tools are used to activate illegally obtained copies of software or crack their intellectual property protection systems, the greater the chances of ending up with a nasty malware infection.

Those who can't afford to purchase a Windows license should look at alternative options instead, such as accepting the limitations of the free version, monitoring for special offers from trustworthy platforms, or using Linux.

Ultimately, users should not trust license activators and any unsigned executable authored and released by unknown vendors to run on your system.

## Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

New stealthy Nerbian RAT malware spotted in ongoing attacks

Microsoft May 2022 Patch Tuesday fixes 3 zero-days, 75 flaws

New NetDooka malware spreads via poisoned search results

- BitRAT
- Microsoft
- RAT
- Remote Access Trojan
- South Korea
- webhards
- Windows 10

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article



## You may also like: