BitRAT malware spreads through Windows activation software

A new BitRAT malware distribution campaign is underway targeting users who want to crack Windows with third-party activation software.

BitRAT is a dangerous remote access trojan that is for sale on hacker forums and dark web for as little as 20 USD for lifetime license.

Therefore, each license buyer has his own approach to distribution, from fraud, exploiting security holes to abusing trojan software.

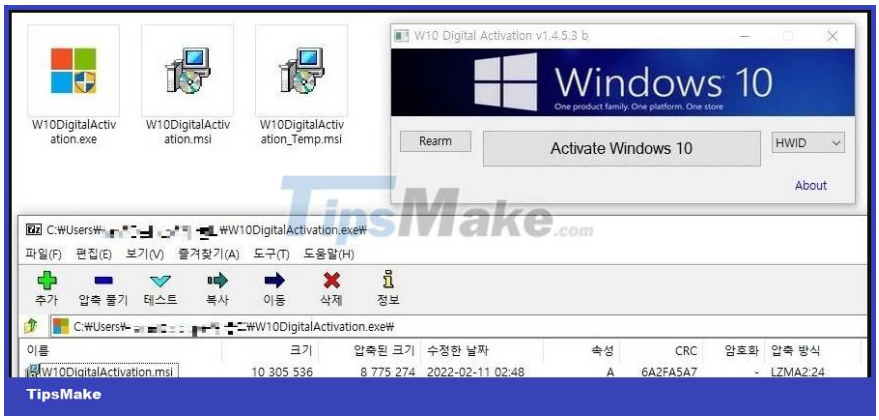
Aimed at people who like to crack software

In a new BitRAT distribution campaign discovered by researchers at AhnLab, hackers distribute malicious code in the form of Windows 10 Pro license activation software on webhards.

Webhards is a popular online storage service in Korea with a steady stream of visitors from direct download links posted on social networks or Discord. Therefore, hackers have taken advantage of the popularity of webhards to spread malicious code.

Based on some Korean characters in the code and distribution, it can be temporarily speculated that the hacker behind the new BitRAT campaign is Korean.

The malware has been named by the hacker as W10DigitalActicting.exe and has a fairly simple interface with just one button "Activate Windows 10". However, instead of activating the Windows 10 license on the victim's machine, the software downloads a malicious code from a command and control server run by the hacker.



Tool interface
The downloaded malware is BitRAT and installed in %TEMP% as "Software_Reporter_Tool.exe" and added to the Startup folder. The downloader also adds exclusions in Windows Defender to ensure that BitRAT goes undetected.

After completing the installation of malicious code, the downloader automatically removes from the system leaving only BitRAT.

A flexible RAT malware

BitRAT is advertised as a powerful, inexpensive, and versatile malware. It can steal valuable information from victim's machine, perform DDoS attacks, bypass UAC.

BitRAT also supports keylog, clipboard monitoring, webcam access, audio recording, web browser credential stealing and XMRig virtual currency mining function.

In addition, it provides remote control of Windows systems, hidden virtual computer networks (hVNC) and reverse proxies via SOCKS4 and SOCKS5 (UDP). In this respect, ASEC analysts have found similarities

between BitRAT and malware such as TinyNuke, AveMaria (Warzone).

Cracked software, potential danger

Using pirated software, crack will put you at high risk of being attacked by hackers. The more tools you install to activate software copyright (crack software/games), the higher your risk of being hacked, having malicious code installed on your computer, or having information stolen.