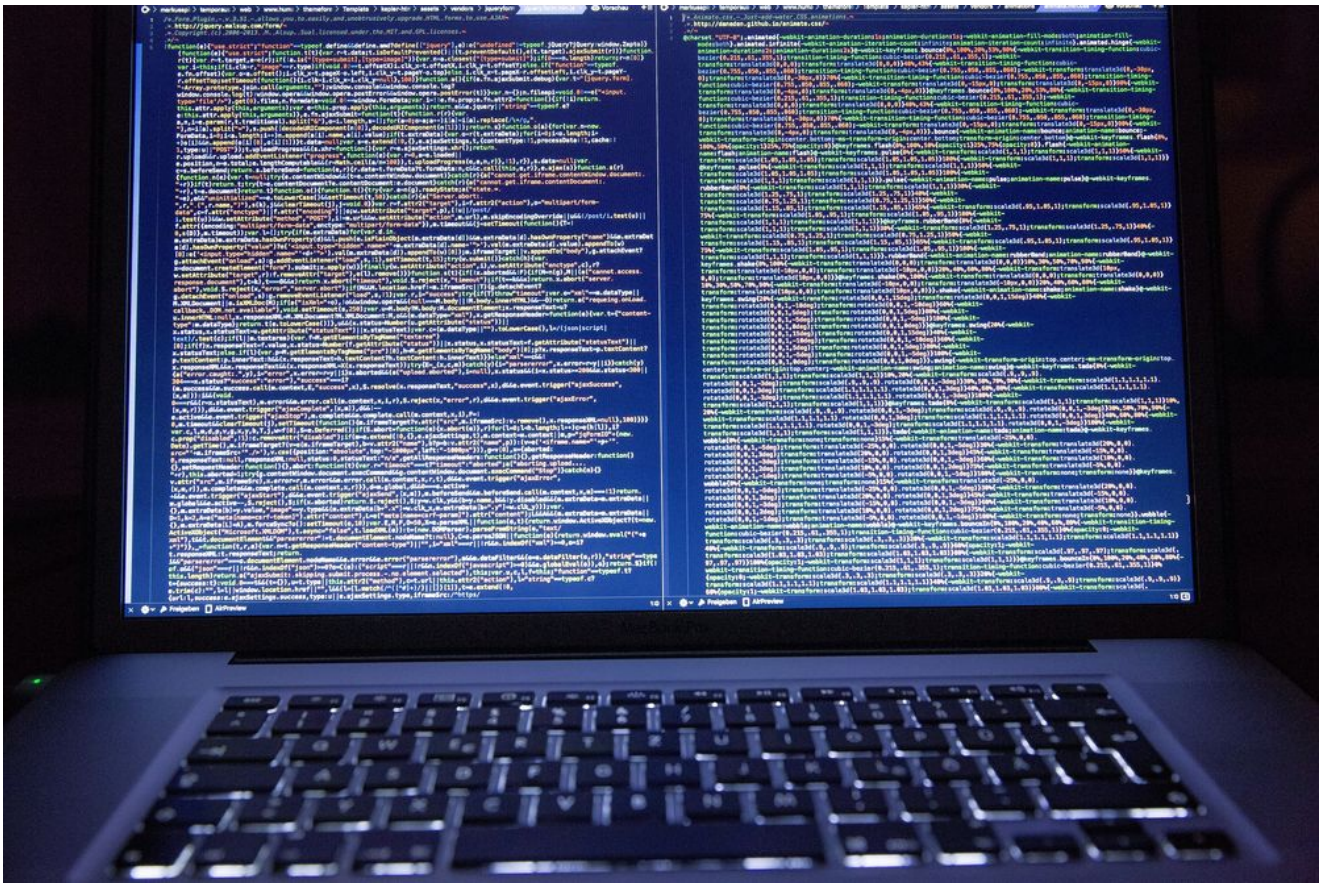
BitRAT Malware Seen Spreading Through Unofficial Microsoft Windows Activators

Industry News
1 min read

Vlad CONSTANTINESCU
March 22, 2022



BitRAT malware has launched a new campaign targeting people who try to activate pirated versions of Windows operating systems for free through unofficial license activators.

The criminals behind the campaign reportedly distribute the payloads in the guise of Windows 10 Pro license activators and push them on webhards, online storage services popular in South Korea.

Webhards are frequently used to create direct download links, which are then posted on communication platforms such as Discord and various social media services. Due to their widespread use and versatility, they have slowly become one of the most pervasive malware distribution channels among hackers.

In the newly discovered campaign, the malicious file, named **W10DigitalActiviation.exe**, mimics a simple, one-button unofficial Windows 10 activator. Upon pressing the faux "Activate Windows 10" button, victims trigger the download of the BitRATpayload, which is then deployed to **%TEMP%** as **Software_Reporter_Tool.exe**,configured to run at excluded from Windows Defender's detection mechanisms.

After the downloader performs the operations above, it deletes itself from the infected computer in an attempt to wipe its tracks.

Judging from the campaign's distribution manner and the presence of Korean characters in some of its code snippets, security experts suspect Korean threat actors are behind the operation.

BitRAT is a notorious remote access trojan (RAT) marketed on underground cybercriminal web markets and forums. Its price tag of $20 for lifetime access makes it irresistible to cybercriminals and helps the malicious payload spread.

Furthermore, each buyer's *modus operandi* makes BitRAT even harder to stop, considering it can be employed in various operations, such as trojanized software, phishing and watering hole attacks.

BitRAT's popularity arises from its versatility. The malicious tool can perform a wide range of operations, including data exfiltration, UAC bypass, DDoS attacks, clipboard monitoring, gaining unauthorized webcam access, credential theft, audio recording, XMRig coin mining and generic keylogging.

TAGS

industry news

AUTHOR

Vlad CONSTANTINESCU

Vlad's love for technology and writing created rich soil for his interest in cybersecurity to sprout into a full-on passion. Before becoming a Security Analyst, he covered tech and security topics.

View all posts