Malicious KMSPico installers steal your cryptocurrency wallets

bleepingcomputer.com/news/security/malicious-kmspico-installers-steal-your-cryptocurrency-wallets/

Bill Toulas

By
Bill Toulas

- December 4, 2021
- 12:06 PM
- 3

Threat actors are distributing altered KMSpico installers to infect Windows devices with malware that steals cryptocurrency wallets.

This activity has been spotted by researchers at Red Canary, who warn that pirating software to save on licensing costs isn't worth the risk.

KMSPico is a popular Microsoft Windows and Office product activator that emulates a Windows Key Management Services (KMS) server to activate licenses fraudulently.

According to Red Canary, many IT departments using KMSPico instead of legitimate Microsoft software licenses are much bigger than one would expect.

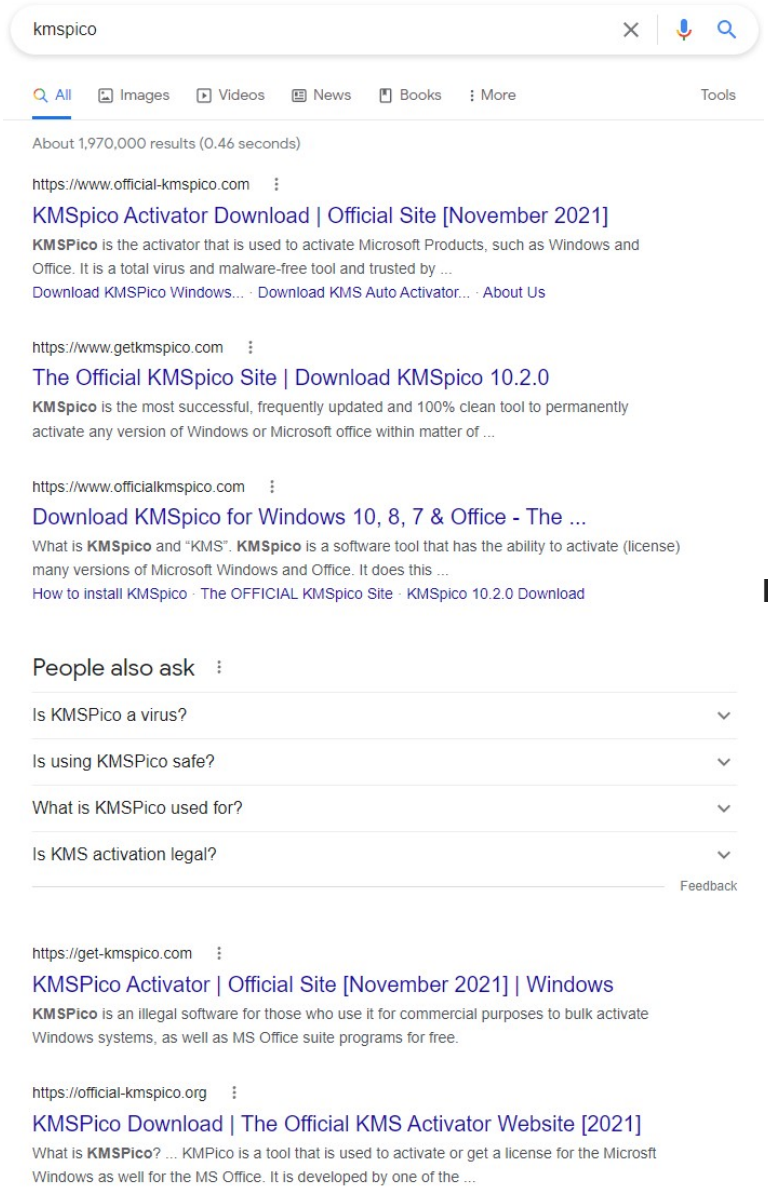
"We've observed several IT departments using KMSPico instead of legitimate Microsoft licenses to activate systems," explained Red Canary intelligence analyst Tony Lambert.

"In fact, we even experienced one ill-fated incident response engagement where our IR partner could not remediate one environment due to the organization not having a single valid Windows license in the environment."

Tainted product activators

KMSPico is commonly distributed through pirated software and cracks sites that wrap the tool in installers containing adware and malware.

As you can see below, there are numerous sites created to distribute KMSPico, all claiming to be the official site.



Most Google Search results are sites that claim to be official

A malicious KMSPico installer analyzed by RedCanary comes in a self-extracting executable like 7-Zip and contains both an actual KMS server emulator and Cryptbot.

"The user becomes infected by clicking one of the malicious links and downloads either KMSPico, Cryptbot, or another malware without KMSPico," explains a technical analysis of the campaign,

"The adversaries install KMSPico also, because that is what the victim expects to happen, while simultaneously deploying Cryptbot behind the scenes."

The malware is wrapped by the CypherIT packer that obfuscates the installer to prevent it from being detected by security software. This installer then launches a script that is also heavily obfuscated, which is capable of detecting sandboxes and AV emulation, so it won't execute when run on the researcher's devices.

```
12859
12860   $dSDOHtQKgnvdgX = 197
12861   $WNvWoHMawKWr = 65
12862   While ((7217-7216)*6709)
12863   Switch $dSDOHtQKgnvdgX
12864   Case 193
12865
12866   $WUtfwvLvtESrU = Execute(XsqTp("89@122@120@111@116@109@79@121@76@114@117@103@122@46@45@88@75@117@1
12867   $56 = 69
12868   For $AhBlwikQcGxTGYLtmgslwSRbcmblHOoGewPnRFZnTumbV = 17 To 27
12869   Local $hwBBRZACWSTmC = 'pmrRynYBzxXmuwTmdqZXUejgGNazWohQIDfgivOUyMHuE'
12870   Local $WUtfwvLvtESrU = Execute(XsqTp("88@121@119@110@115@108@78@120@75@113@116@102@121@45@44@114@7
12871   Next
12872
12873   $dSDOHtQKgnvdgX = $dSDOHtQKgnvdgX + 1
12874   Case 194
12875
12876   $QOtEDYIPsdwYyhNE = XsqTp("117@106@101@101@98@109@104@76@105@73@114@83@119@71@114@108@77",1)
12877   $165 = 157
12878   For $FcYNUgBcTfgZmFeQhGMkpByZQrvVNwQpSofJGZWmDoJJzQ = 12 To 23
12879   Local $pnjkzGeyHYARp = 'IBxGYEWNLVhTxVEuHeIdVItyYDkEFJAZjfaKssHFjvNdYmkiA'
12880   Local $QOtEDYIPsdwYyhNE = Execute(XsqTp("68@114@105@118@101@71@101@116@83@101@114@105@97@108@40@39@
12881   Next
12882
12883   $dSDOHtQKgnvdgX = $dSDOHtQKgnvdgX + 1
12884   Case 195
```

Obfuscated code of Cryptbot

Source: Red Canary

Moreover, Cryptobot checks for the presence of "%APPDATA%\Ramson," and executes its self-deletion routine if the folder exists to prevent re-infection.

The injection of the Cryptbot bytes into memory occurs through the process hollowing method, while the malware's operational features overlap with previous research findings.

In summary, Cryptbot is capable of collecting sensitive data from the following apps:

- Atomic cryptocurrency wallet
- Avast Secure web browser
- Brave browser
- Ledger Live cryptocurrency wallet

- Opera Web Browser
- Waves Client and Exchange cryptocurrency applications
- Coinomi cryptocurrency wallet
- Google Chrome web browser
- Jaxx Liberty cryptocurrency wallet
- Electron Cash cryptocurrency wallet
- Electrum cryptocurrency wallet
- Exodus cryptocurrency wallet
- Monero cryptocurrency wallet
- MultiBitHD cryptocurrency wallet
- Mozilla Firefox web browser
- CCleaner web browser
- Vivaldi web browser

Because Cryptbot's operation doesn't rely on the existence of unencrypted binaries on the disk, detecting it is only possible by monitoring for malicious behavior such as PowerShell command execution or external network communication.

Red Canary shares the following four key points for threat detection:

- binaries containing AutoIT metadata but don't have "AutoIT" in their filenames
- AutoIT processes making external network connections
- findstr commands similar to findstr /V /R "^ … $
- PowerShell or cmd.exe commands containing rd /s /q, timeout, and del /f /q together

In summary, if you thought that KSMPico is a smart way to save on unnecessary licensing costs, the above illustrates why that's a bad idea.

The reality is that the loss of revenue due to incident response, ransomware attacks, and cryptocurrency theft from installing pirated software could be more than the cost of the actual Windows and Office licenses.

Related Articles:

New cryptomining malware builds an army of Windows, Linux bots

Popular NFT marketplace Rarible targeted by scammers and malware

New powerful Prynt Stealer malware sells for just $100 per month

New malware targets serverless AWS Lambda with cryptominers

Verblecon malware loader used in stealthy crypto mining attacks

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.