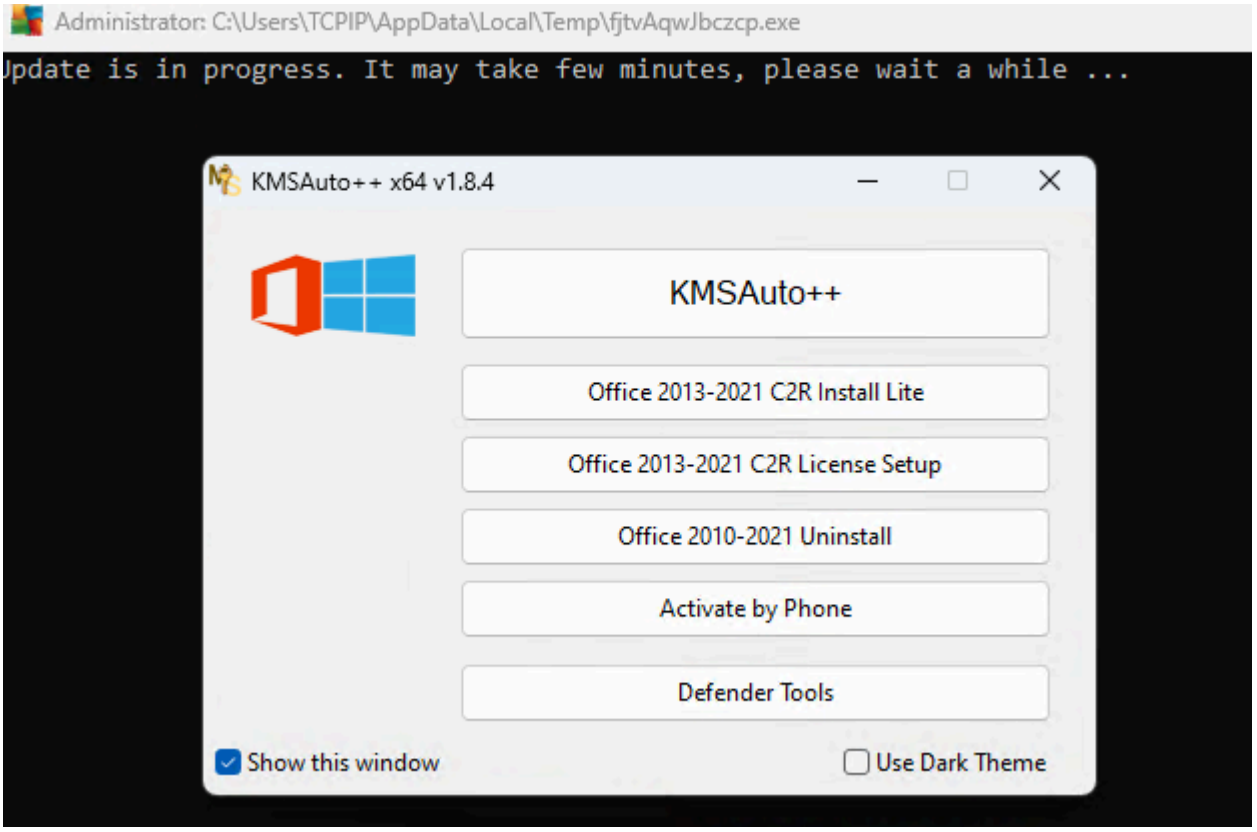
Sandworm APT Exploits Trojanized KMS Tools to Target Ukrainian Users in Cyber Espionage Campaign

By Ddos

Published: 2025-02-12 · Archived: 2026-04-05 20:06:33 UTC



Execution of Trojanized KMS Auto Tool | Source: EclecticIQ

The notorious Sandworm APT (APT44), a Russian-state-sponsored threat actor affiliated with the GRU (Russia's Main Intelligence Directorate), has been observed actively targeting Ukrainian Windows users through trojanized Microsoft Key Management Service (KMS) activators. According to a recent EclecticIQ report, this campaign has been ongoing since late 2023, leveraging pirated software to deliver a new version of BACKORDER, a loader that ultimately deploys Dark Crystal RAT (DcRAT), facilitating cyber espionage and data exfiltration.

The threat actors are disguising malware within a fake KMS activation tool, KMSAuto++x64_v1.8.4.zip, uploaded to torrent sites to target users attempting to bypass Windows licensing. EclecticIQ analysts noted: *"Ukraine's heavy reliance on cracked software, including in government institutions, creates a major attack surface."*

Microsoft has estimated that 70% of software in Ukraine's state sector was unlicensed, providing adversaries like Sandworm an opportunity to distribute trojanized software widely.

How the Attack Works

Step 1: Execution of Trojanized KMS Activator

Upon execution, the fake KMS activation tool displays a Windows activation interface, while in the background, the BACKORDER loader initializes, executing malicious operations without raising red flags.

Step 2: Disabling Windows Defender

The BACKORDER loader executes the following PowerShell command:

powershell.exe -Command Add-MpPreference –ExclusionPath <Folder-Path>

This adds an exclusion rule to bypass security detections, paving the way for malware installation.

Step 3: Deployment of Dark Crystal RAT (DcRAT)

The malware decodes a Base64-encoded domain string stored in its Portable Executable (PE) file and downloads DcRAT from *kmsupdate2023[.]com/kms2023.zip*. The RAT is then stored and executed from:

- \AppData\Roaming\kms2023\kms2023.exe
- \AppData\Local\staticfile.exe

Step 4: Establishing Persistent Access

To ensure longevity on the infected system, DcRAT creates multiple scheduled tasks using Windows' built-in binary *schtasks.exe.* This enables persistence across reboots.

Once executed, DcRAT exfiltrates sensitive data, including:

- Screenshots of the device
- Keystrokes recorded from the victim
- Browser cookies, history, and saved credentials
- Stored FTP credentials
- System information (hostname, installed applications, language settings, etc.)
- Saved credit card details

According to EclecticIQ, "*DcRAT kms2023.exe establishes a remote connection to the command-and-control server onedrivepack[.]com/pipe_RequestPollUpdateProcessAuthwordpress.php, that is very likely operated by the threat actor*."

Multiple pieces of evidence link this campaign to Sandworm (APT44), including:

1. Use of ProtonMail WHOIS records
2. Overlapping C2 infrastructure
3. Reuse of BACKORDER and DcRAT malware
4. Russian-language debug symbols in malware samples

Organizations and individuals must exercise extreme caution when downloading software from untrusted sources and should implement security best practices.

Related Posts:

- Mandiant Unveils Russian Cyber Espionage in Ukraine's Grid Disruption
- Sandworm Targets Ukraine's Critical Infrastructure with New Attack Wave

Support Our Threat Intelligence

If you find our CVE report and cybersecurity news helpful, consider supporting our work.

Post navigation
