

Phishing Attacks Leverage TikTok, Instagram Reels

 reversinglabs.com/blog/social-media-attacks-phishing

Zaria Vuksan

June 9, 2026

RL has discovered two social engineering attack techniques targeting users via short-form videos. Here's how they work.

Social Engineering Attacks Target One Tutorial at a Time

Short-form videos on social media apps are currently being leveraged by threat actors as a phishing vector, utilizing tutorial style content with the promise of free premium software to lure victims onto malicious sites.

This is an important threat to be cognizant of, as the videos can trick users into directly downloading malware. In order to best defend organizations, steps can be taken to mitigate the risks associated with these videos, both in user training and technical guardrails.

Here's what these malicious videos look like, how they work — and why they are so successful. ReversingLabs (RL) analyzed the phenomena's two distinct campaigns, which both managed to reach a large audience by leveraging different metrics to game the content recommendation algorithms.

The Campaigns

If you've used social media, you know that sometimes it recommends solutions to problems you never thought about solving. Most of the time, you don't need these problems solved, but sometimes you stumble across something actually useful. Someone offers you an easy way to get free software, like Spotify Premium or Microsoft Word. The video looks like everything else you've seen during your scroll, and those thousands of views and hundreds of likes have to count for something.

Unfortunately the algorithm and your trust in social media has signed you up for malware, with the likes of [Vidarstealer](#) on the table. The tutorial was too good to be true and now a mess is on your hands.

During RL researcher's investigation of malicious social media videos, two different lure techniques were observed across accounts and social media platforms. Primarily conducted on TikTok and Instagram Reels, these campaigns use the same template to mass produce videos and make regular posts. Either approach is a means to a different end, and the differences demonstrate how attackers can leverage different aspects of social media engagement to reach more potential victims.

One methodology involves fake tutorials for software installs, with professional sounding voice overs and clean graphics. The second approach relies on posts demonstrating how to use premium software for free, spanning multiple videos, with a centralized tutorial being introduced after the account gains traction. Regardless of the differing hooks, both campaign tactics seek to drive viewers to a secondary website hosting free software of dubious intent.

Method One: Malicious Tutorials

The malicious tutorial campaigns come from a myriad of almost identical accounts, with usernames like “windows.tips” or “windows.insights” and the same blue and white profile picture.

 screenshot of the malicious user, showing their profile picture: A blue outline of a crown on a white background.



Figure 1.1, screenshot of the malicious user, showing their profile picture: A blue outline of a crown on a white background.

The profile picture uses this color palette to mirror the legitimate Window’s social media account’s icon. This may help establish credibility for the malicious account.

 screenshot of the official windows account, showing their profile picture: A blue Windows logo on a white background.



Figure 1.2, screenshot of the official windows account, showing their profile picture: A blue Windows logo on a white background.

The videos utilize descriptions and tags to make them seem like legitimate customer support pages.

 image showing the various search tags utilized by the malicious account.



Figure 1.3, image showing the various search tags utilized by the malicious account.

Here is an example of what one of their tutorials may look like.

In this video, a potentially AI-generated voice reads out simple directions to unlock Spotify Premium. The video is short and to the point, showing users step-by-step how to access Powershell from the Windows menu, and what command to input to supposedly unlock this free service. A non-technical user does not know any better, and may assume it is legitimate. Attackers are relying on this lack of understanding. The *iex irm* command will download

scripts present at the specified address, and some users may believe the `msget[.]run/spotify` is a Microsoft-affiliated or otherwise legitimate domain. Social media users executing this command may trust the video on face value, without verifying what is being downloaded when they run this command.

What makes the video dangerous is how clean and professional it is, creating a false sense of authority. Tutorials are frequently liked and saved, as users want to save them for later viewing. Saving is a very valuable interaction to posts, and the act causes the social media platform algorithm to push the content to more users. Users may also share the tutorial, creating more engagement which the content serving algorithm favors. Highly successful videos have many likes, shares and saves. The following video is one such example, with over 100,000 views and thousands of interactions. Most users default to liking videos, which makes it a milder indicator of quality to the algorithm as opposed to the more selectively used save, share and comment. The fact the following video has nearly 200 more saves as opposed to likes proves how threat actors are targeting the more algorithmically valuable form of engagement through these videos.

 Image of video with 1,699 saves, 1,581 likes, and 974 shares. Not shown on this screen is that the video has 109,000 views.



Figure 1.4, Image of video with 1,699 saves, 1,581 likes, and 974 shares. Not shown on this screen is that the video has 109,000 views.

In the case a user does follow the directions described in the video tutorial, they will most likely end up with an unfortunate surprise on their device. Researchers extracted the executable at the `msget[.]run/spotify` domain, and used ReversingLabs Spectra Analyze for a deeper look.

 Spectra Analyze results for the executable from the `msget[.]run` domain.



Figure 1.5, Spectra Analyze results for the executable from the `msget[.]run` domain.

The `build.exe` file delivered through this command is identified as Vidarstealer, confirming other reports of this phenomenon. Vidarstealer is a popular infostealer malware as a service (MaaS) offering which steals credentials, financial information, and tokens from victims. It is a long standing malware that was updated in October of last year, making it more evasive and stable. With an affordable \$300 lifetime license, it is a much-used tool by malicious actors. This can be seen with its usage across various campaigns, like [fake game cheats](#), [malvertising](#), and more. The attackers using this malware seem to be targeting a variety of demographics and regions, with many targets being individual users. The ease of use of

MaaS combines with the accessibility of social media as a vector, making a dangerous combination.

Method Two: More Than Just Flexing

The second type of video found has a completely different approach. Gone is the professionalism. Now, the focus is short videos blasting trending music while scrolling through the features of premium software, mainly Spotify Premium. There is text on screen, which usually claims they got these premium features for free. This video category is posted by accounts that look like a typical user. However, their library of posts consist entirely of copy/paste videos solely about their free Spotify Premium experience.

 screenshot of videos of the Spotify app with the caption, as seen in a sample lure video posted on TikTok.



Figure 2.1, screenshot of videos of the Spotify app with the caption, as seen in a sample lure video posted on TikTok.

It seems strange upon first glance, but one look into the comment section reveals their goal. These vague videos get users to ask questions, pondering how the poster was able to get free access to the program. It is a natural aspect of human curiosity. Unfortunately, this curiosity plays right into what the attacker wants. This becomes more evident with some of the videos, which encourage users to comment with certain phrases.

 Screenshot of video encouraging users to comment “ok”.



Figure 2.2, Screenshot of video encouraging users to comment “ok”.

This commenting strategy is used by non-malicious creators, such as recipe writers, to help build engagement and foster an audience relationship. After viewers comment, the creator messages or replies with directions. Attackers use this technique and trust in it to provide directions to dangerous sites. If not using the previously mentioned comment reply approach, they will redirect users to a separate tutorial video or a link in their account description, in order to funnel victims to malicious sites. Regardless of how the tutorial is delivered, the content strategy revolves around generating user comments for engagement to boost videos, then building a rapport before providing the malicious tutorial.

Once the attacker gathers the interest from their audience, they release the coveted techniques. This involves links to sites advertised to contain the free software downloads. Some of these sites, like *pluginchad[.]xyz* or *maxapk[.]xyz*, have been taken down. However,

researchers were able to explore the *d4ug[.]site* (now inactive) using Spectra Analyze's Interactive Sandbox.

 D4ug[.]site, which claims to “Unlock premium games & AI tools”. Some examples of the offerings are Spotify Premium, CapCut Pro, and YouTube Premium.



Figure 2.3, D4ug[.]site, which claims to “Unlock premium games & AI tools”. Some examples of the offerings are Spotify Premium, CapCut Pro, and YouTube Premium.

The website has many offerings of memberships and software. Clicking the Spotify Premium option brings up the screen below.

 Download screen for Spotify Premium, with a list of 5 tasks to do to unlock the download.



Figure 2.3, Download screen for Spotify Premium, with a list of 5 tasks to do to unlock the download.

The first two options were attempted, leading to surveys:

 the first page of two surveys, advertising free gift cards.



Figures 2.4.1 and 2.4.2, the first page of two surveys, advertising free gift cards.

Researchers were unable to successfully complete surveys utilizing dummy information.

 End of the surveys, saying users did not qualify.



Figures 2.5.1 and 2.5.2, end of the surveys, saying users did not qualify.

With the surveys unsuccessful and other options not possible, researchers were unable to confirm the existence of the Spotify install, much less determine what it may be. Regardless of any payload delivery, it's clear these techniques can be used to drive traffic to any site, which can easily be something dangerous.

The Social Media Angle

It is clear attackers understand how to make successful content. Using social media is free and rewards frequent uploads. By using multiple platforms, accounts, and posts, attackers are able to access many users. Focusing their content into techniques that drive engagement only furthers their reach. Engagement can be encouraged through the nature of tutorials being

saved and shared by users, or with techniques like asking for comments. Running a social media account is a very low time investment endeavor, and with AI voice and video generation, videos are becoming easier to mass produce. Social media provides ample opportunities for attackers to access victims, and it is likely there will be increasing numbers of these accounts and videos in the coming years.

The unfortunate thing is that these techniques work, with hundreds of thousands of views, thousands of saves, likes, and shares, and hundreds of comments. Comments, shares and saves are hugely influential on how well content performs, and these techniques leverage that priority. These videos clearly do reach a large audience.

In addition to being an effective way to spread malicious content, social media videos are hard to defend against, like any social engineering technique. Users who catch onto the malicious intent, either through research or falling for it themselves, may try to warn others in the comments. However, most platforms allow for creators to delete comments and block commenters, so diligent attackers can snuff out this resistance. Reporting videos is not a reliable way to get action taken either. Researchers attempted to report posts on Instagram as scams, but the reports were rejected. Platform responses to reports are inconsistent, and even if a report gets to a human reviewer, said reviewer may not be qualified to understand the ramifications of these malicious videos. Even when a social media video or account is taken down, it is likely only after they have amassed a large amount of views, and threat actors can easily just start anew.

Why This Type of Attack is Important

This kind of social engineering is an easy way for threat actors to drive traffic off social media and onto an attacker-controlled malicious website. Malware-as-a-service offerings make it extremely easy for people with any level of skill to profit off the exploitation of others, and the accessibility of social media makes the methodology detailed in this analysis a highly attractive way for threat actors to push malware. There are likely many more variations of videos with the same intentions. People are looking for scams in their email inboxes and text messages, but not as much on their social media feed. Especially when these posts are under the guise of being helpful, rather than the urgency or sob stories associated with stereotypical phishing attempts. These videos can pop up at any time, so it is important that organizations stay prepared.

One of the key defenses against this kind of attack is to regularly audit permissions, ensuring people with installation privileges understand what they are installing. Most of these examples described in this analysis are leisure software, but they are not exclusively so. Some promise access to professional software, which employees may deem useful enough to attempt to use

on work devices. Phishing training also needs to be maintained and up to date, so people are aware of the evolving threat landscapes. Organizations must broaden their awareness of a variety of vectors, and focus on more than just typical avenues of phishing. Users are encouraged to report suspicious social media advice even when using personal social media on personal devices. The more reports, the more likely it is that the accounts are taken down, which does slow down the momentum of these attackers. Remaining diligent can help everyone be safer.

Short-Form Attacks Are Long on Risk

Short-form video platforms are being used by threat actors to encourage users to take risky actions. These actions may result in users downloading malicious content or giving up personal information to unsafe sources. Threat actors use tactics to increase the amount of engagement their posts get, spreading the harmful content across the website. This method is difficult to counter, since attackers can delete comments warning of the scams, and platforms are unlikely to intervene when content is reported. This leaves it on organizations to regularly audit permissions and train their staff to prevent these situations from occurring.

Indicators of Compromise

Hashes:

03bbc4fa1fd784276da135ab62fef85aaddea66e6eb176d7e59c3398f818b153

Domains:

Pluginchad[.]xyz

Maxapk[.]xyz

D4ug[.]site

SImgr[.]sh

Ms[.]get

sImgr[.]sh

Accounts:

tiktok[.]com/@windows.tips1

tiktok[.]com/@windows.insight

tiktok[.]com/@davidcooksey47

tiktok[.]com/@tracyhughe

tiktok[.]com/@mr.capcut.pro2

instagram[.]com/wtips404

instagram[.]com/wndwstips

instagram[.]com/epemberton369

Tags: [Threat Research](#) [Researcher's Notebook](#)

Topics



Why RL Built Spectra Assure Community

Why RL Built Spectra Assure Community

We set out to help dev and AppSec teams secure the village: OSS dependencies, malware, more. Learn how.

[Read More about Why RL Built Spectra Assure Community](#)

[Why RL Built Spectra Assure Community](#)

Subscribe

Get the best of RL Blog delivered to your in-box weekly. Stay up to date on key trends, analysis and best practices across threat intelligence and software supply chain security.