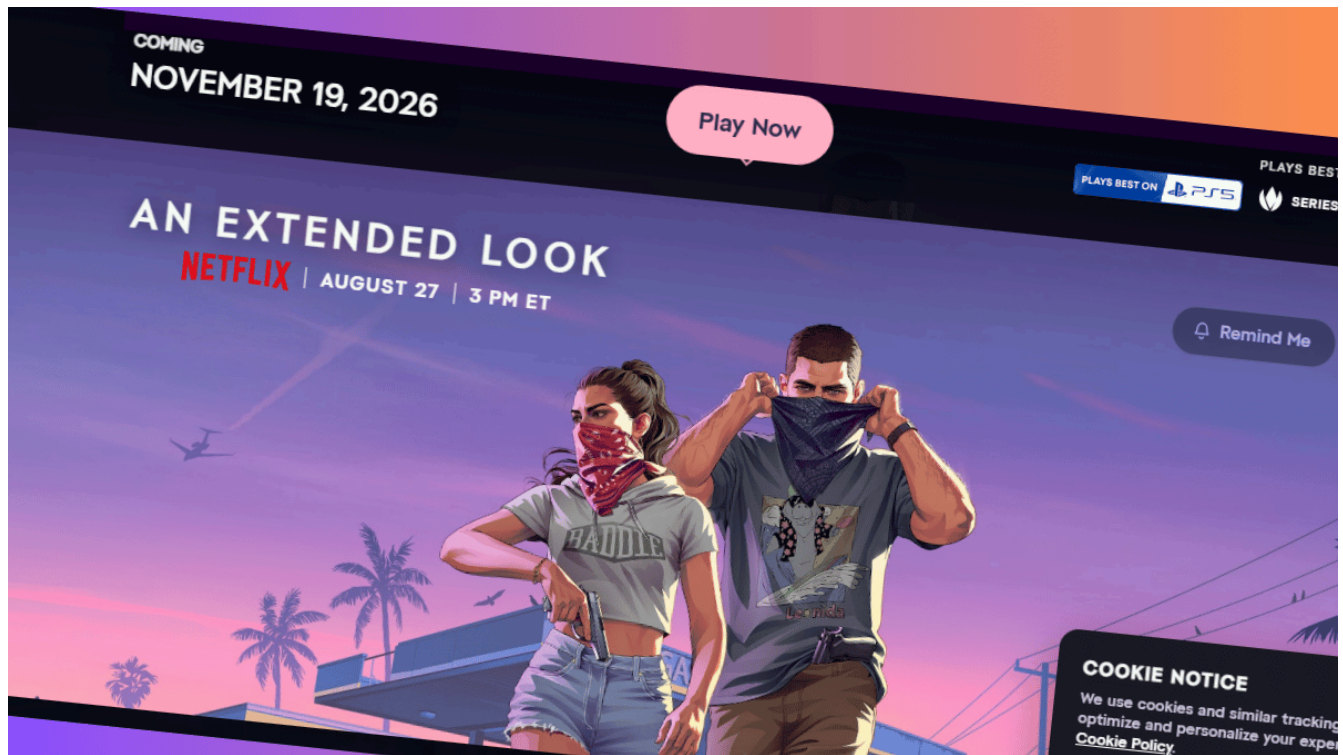


Fake GTA 6 Extended Look and demo sites deliver an infostealer

malwarebytes.com/blog/threat-intel/2026/08/fake-gta-6-extended-look-and-demo-sites-deliver-an-infostealer

Stefan Dasic

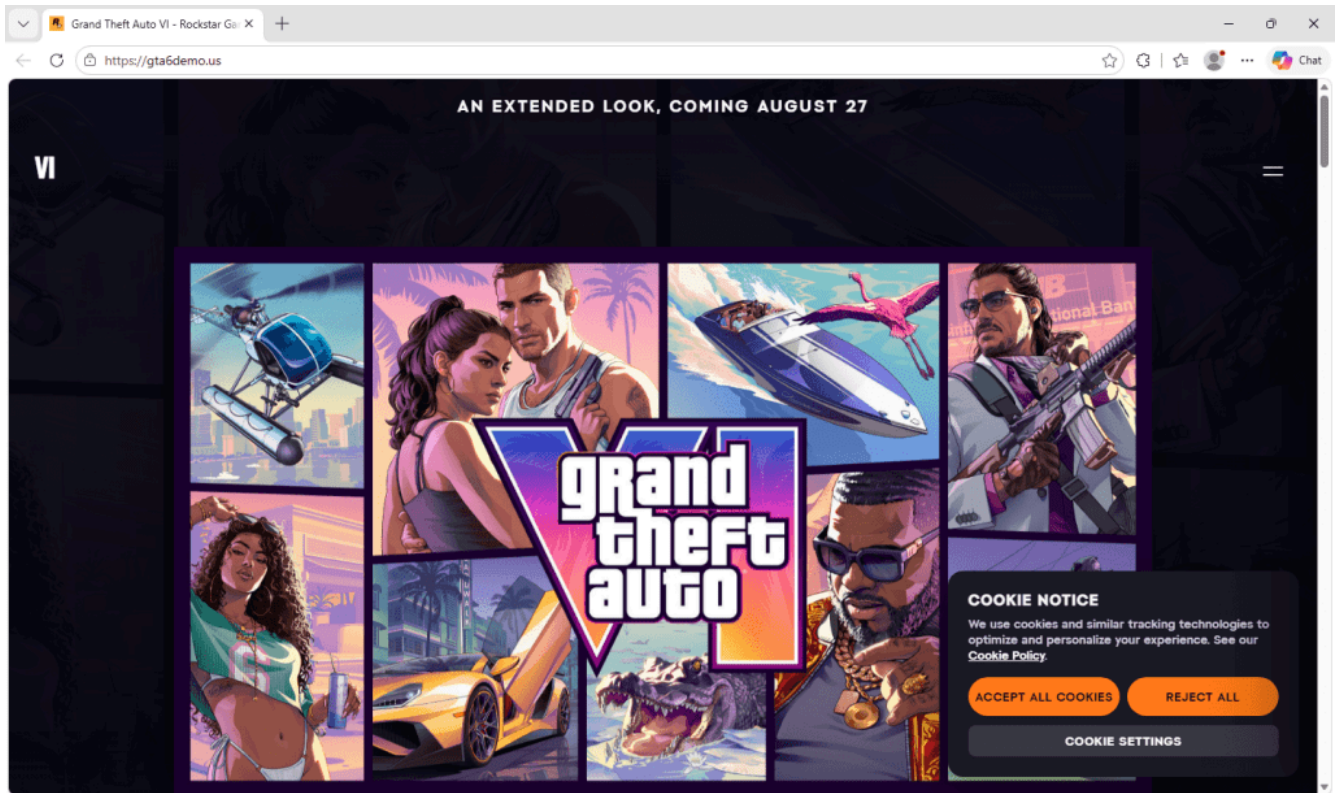
August 24, 2026



GTA 6 footage really has leaked online, and Rockstar has an official Extended Look coming to Netflix on August 27. But cybercriminals are exploiting the hype with fake Rockstar sites that lead visitors to password-stealing malware.

We identified a network of sites appearing in searches for a GTA 6 demo and impersonating Rockstar Games. One Google result advertises an “Official Download,” but visitors who follow the sites’ “Play Now” links can instead end up downloading `gta6_installer.exe`.

The sites are particularly convincing because they copy Rockstar’s genuine promotion for its August 27 extended look at GTA 6. But the executable they deliver isn’t a demo, game, or video. It’s an information stealer designed to take passwords stored in browsers, cookies, and authenticated sessions. And because stolen browser sessions can sometimes be reused without going through the normal login process, even two-factor authentication (2FA) may not be enough to stop them.



One of the fake GTA 6 demo websites impersonating Rockstar Games

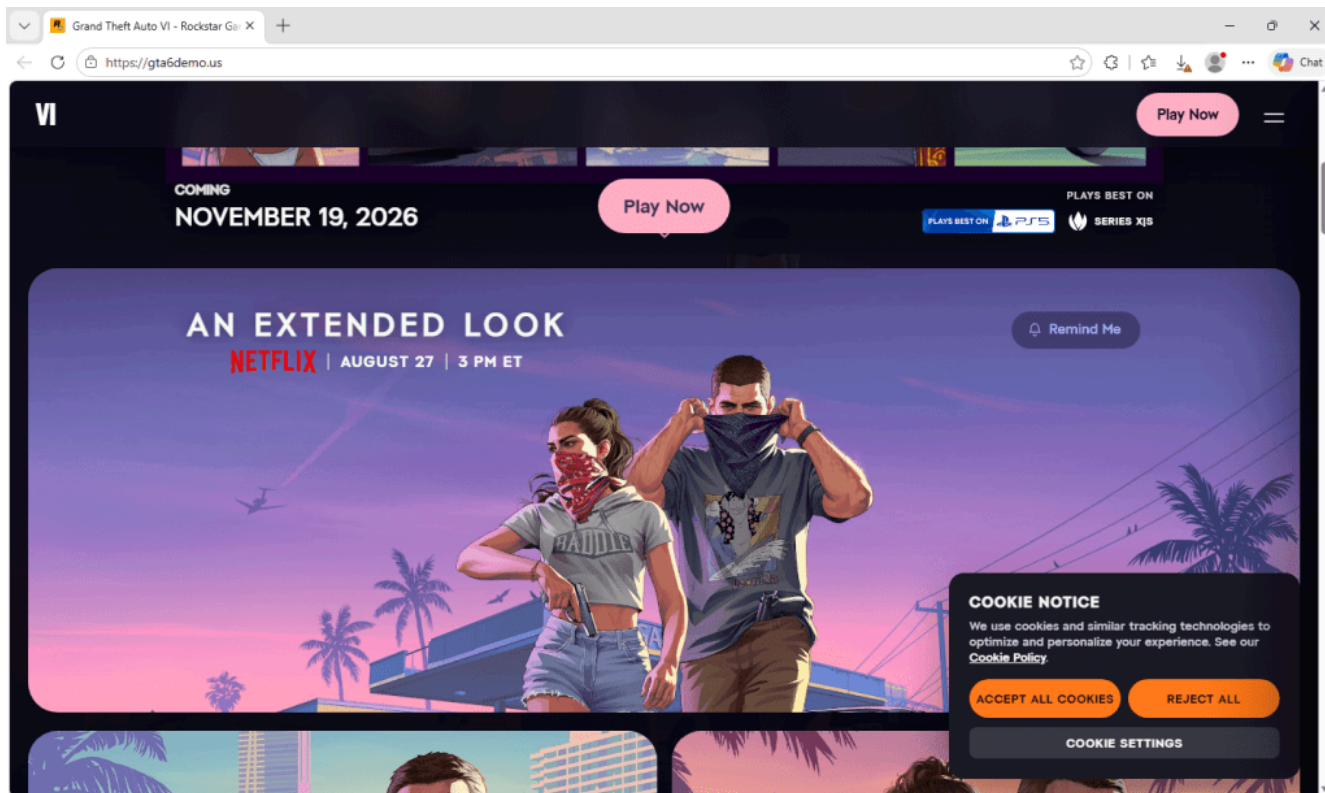
There is no GTA 6 demo

Rockstar has not announced or released a demo of Grand Theft Auto VI.

The game is scheduled for release on November 19, 2026, for PlayStation 5 and Xbox Series X|S. Rockstar has not announced a PC version.

Rockstar has announced an extended look at GTA 6 for August 27, premiering on Netflix before appearing on its YouTube channel later that day. **That's something to watch, not a playable demo or game download.**

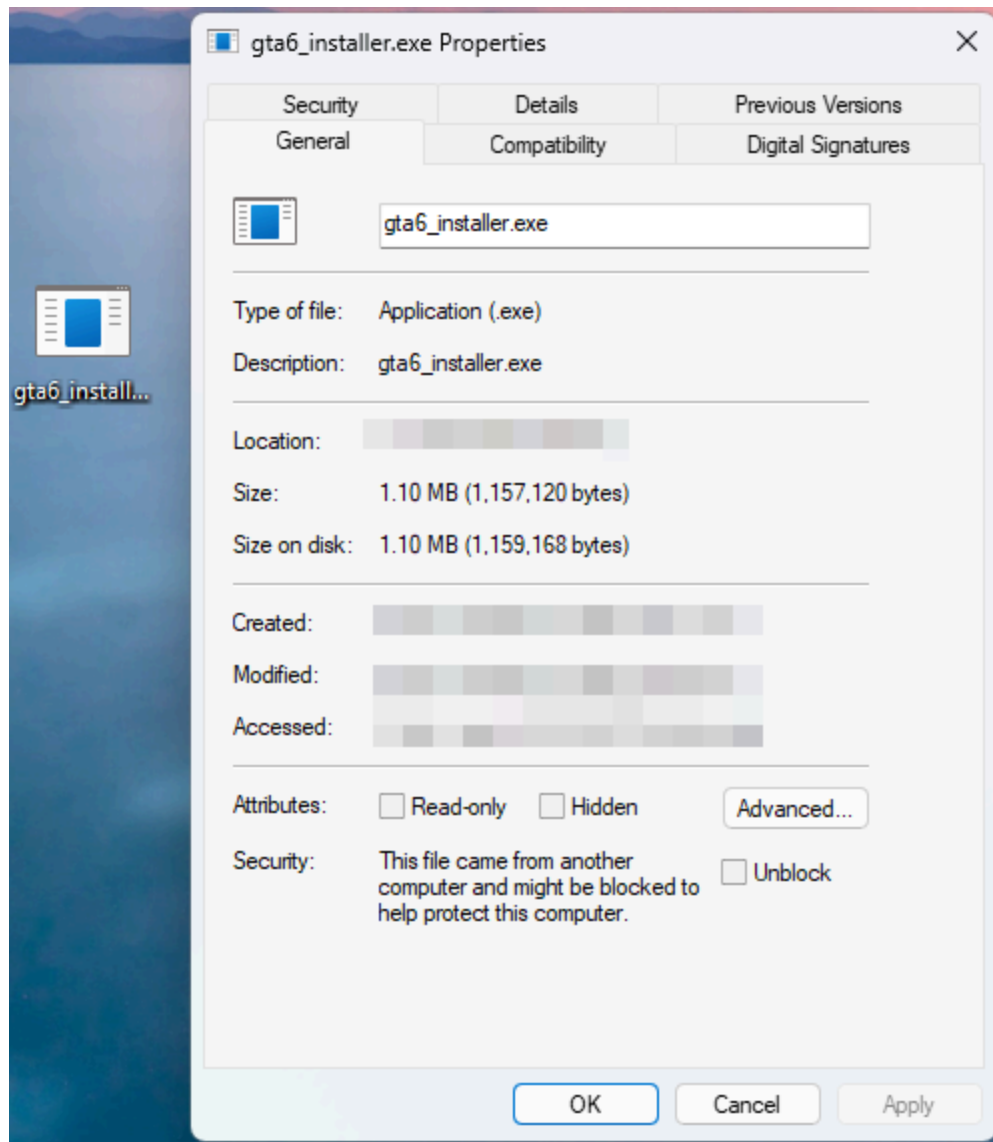
The scam sites copy this genuine announcement while using "Play Now" buttons that can lead visitors to the malicious executable.



The site copies Rockstar's genuine Extended Look promo, but adds a fake "Play Now" button

In other words, there is no legitimate GTA 6 demo or PC build to download. This isn't the first fake GTA 6 offer we've seen. Earlier this year, scammers were charging people hundreds of dollars for [fake GTA 6 early access](#).

The file size should also immediately raise suspicion. The executable delivered by these sites is just 1.1 MB. That is nowhere near enough to contain a modern AAA game. In fact, the screenshot we took of one of the websites is larger than the file it was offering.



The supposed GTA 6 installer is just 1.1 MB

The leak created the opening

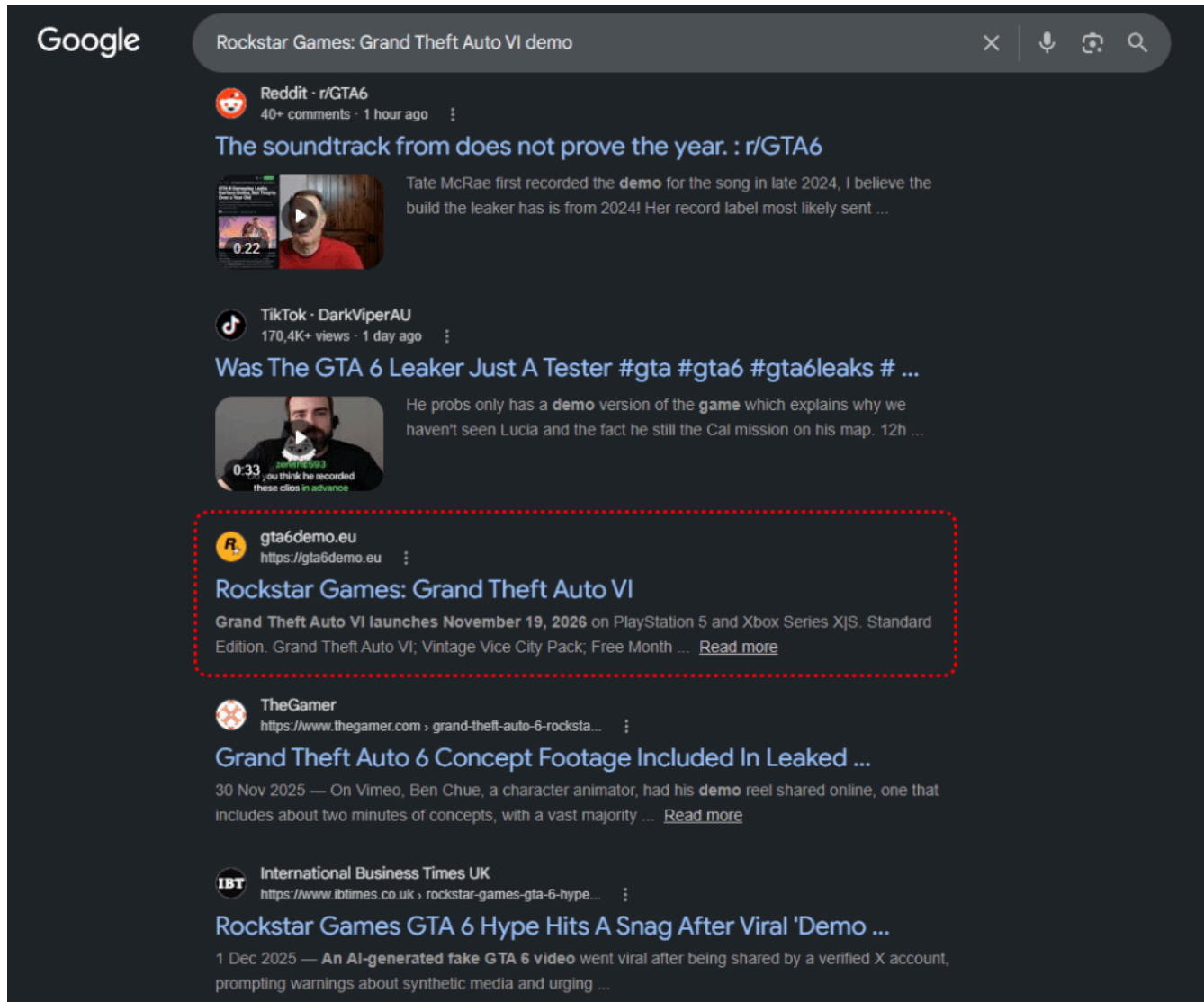
On August 18, new GTA 6 gameplay footage and what appears to be a complete map of Leonida, the game's setting, began circulating online. A person or group calling itself Cyberleek claimed responsibility.

Rockstar and Take-Two responded with takedowns, with Take-Two filing DMCA subpoenas seeking records from Microsoft and Discord that could help identify whoever is behind the leaks.

The malicious `gta6_installer.exe` sample was first spotted on August 19, just one day after the first Cyberleek material began circulating.

Apparently genuine unauthorized GTA 6 material was already circulating, giving people searching for leaked footage, maps, or unofficial builds reason to believe there might be more out there.

But genuine leaks weren't the only thing competing for that attention. Leaked clips carried promotional material for a cryptocurrency token associated with Cyberleek, while Cyberleek's website solicited cryptocurrency donations and offered paid advertising placements in future GTA 6 videos. AI-generated and recycled footage was also being presented on social media as fresh leaks.



One of the fake GTA 6 sites appearing in Google search results alongside legitimate GTA 6 coverage

This isn't the first time GTA 6 has been caught up in a major leak. [In 2022](#), Rockstar confirmed that an attacker had stolen and published development footage of the game.

Leaks create exactly the kind of environment malware operators can exploit: huge demand for unofficial material, mixed with fakes, promotions, scams, and genuine leaks that can all be

made to look remarkably similar.

The fake GTA 6 demo is another part of that ecosystem, but one designed to steal passwords and logged-in browser sessions.

What the file actually does

The installer belongs to the Vidar family, a well-established infostealer [we've seen](#) in other recent malware campaigns that is sold as a service to cybercriminals. Malwarebytes detects this sample, and blocks the websites and network infrastructure associated with the campaign.

Vidar is designed to steal the information browsers remember for you. That could give attackers access to accounts including your email, social media, gaming, and shopping accounts.

In this sample, it went looking for:

- Saved passwords and login details
- Session cookies
- Browsing and download history
- Autofill and other saved browser profile data
- Credentials stored by FTP clients

Our analysis showed 19 browser targets, including Chrome, Edge, Firefox, Brave, Opera, and Vivaldi. It also searched Thunderbird profile directories and targeted Perplexity's Comet browser and the WebView2 browser embedded inside Roblox Studio.

The behavior report showed no persistence mechanism designed to make the malware survive a reboot. We observed no startup entry, scheduled task, or installed service that would relaunch it automatically.

But an infostealer doesn't need to remain on your computer to cause lasting damage. Once passwords or session tokens have been stolen, attackers can continue trying to use them after the malware itself is gone.

That is one reason an infection can be easy to miss. In our analysis, it produced no visible user-facing window and installed nothing that a user would normally notice. From the victim's perspective, the supposed GTA 6 installer may simply appear to do nothing.

Why changing your password might not be enough

If you use a password manager and unique passwords, you might assume there is little useful information for a stealer to take directly from your browser.

Session cookies change that.

When you sign in to a website, the site gives your browser a session token that tells it you have already authenticated. That is why you do not have to enter your password every time you open another page.

If an attacker steals a usable session token, they may be able to reuse that authenticated session without going through the normal login process again.

That matters for 2FA too. 2FA protects the login process, but a stolen session was created after that login had already succeeded. Depending on the service and its security controls, an attacker may therefore be able to reuse the session without being asked for your password or 2FA again.

This is why changing your password after a stealer infection may not be enough by itself. A password change does not necessarily invalidate every existing session.

You should also use the service's option to sign out everywhere, revoke active sessions, or remove unfamiliar devices.

How to protect yourself

- **Check it's official.** Do not assume an unofficial "demo," beta, early build, or leaked version is legitimate just because a game has not launched yet. Check the publisher's official website and store pages first.
- **Use official download sources.** Download games and demos only from official sources such as Steam, the Epic Games Store, PlayStation Store, Xbox, or the publisher's own website.
- **Check the file size.** A one-megabyte executable cannot contain a modern AAA game.
- **Don't trust search results.** Attackers can buy advertisements and optimize malicious pages for exactly the terms people search during major news events.
- **Don't trust appearances.** Official artwork, logos, screenshots, and page layouts are easy to copy.
- **Be careful with leaked material.** By definition, there is no official distribution channel to tell you which download is genuine. If what you want is GTA 6 footage, Rockstar's official Extended Look arrives on August 27.

- **Block malicious sites.** [Malwarebytes Browser Guard](#) blocks malicious pages like these before they load, helping stop the attack before a download ever reaches your computer.

What to do if you ran it

If you downloaded and ran a supposed GTA 6 demo installer, assume credentials and active browser sessions on that computer may have been compromised.

Work through the following steps:

1. **Scan the affected computer** with [Malwarebytes](#) or another trusted security product and remove anything it detects.
2. **Use a clean device to change important passwords**, starting with your primary email account, followed by banking, payment services, and accounts tied to your identity.
3. **Sign out of active sessions everywhere you can.** Look for options such as “sign out everywhere,” “log out of all devices,” or “active sessions.” This is what deals with stolen session cookies and tokens.
4. **Check your accounts for changes you did not make**, including new email forwarding rules, recovery addresses, phone numbers, authorised applications, and unfamiliar devices.
5. **Enable two-factor authentication** on accounts that don’t already have it.
6. **Monitor important accounts closely** for unusual activity over the following weeks.

Check gaming accounts as well. Steam, Epic, and similar accounts can contain saved payment methods, valuable inventories, and access to other services.

Technical details

It uses your own browser to unlock your data

Browsers increasingly use stronger encryption and application-level protections for saved passwords and cookies. In particular, Chromium-based browsers have made it harder for unrelated software to simply copy a database and decrypt everything directly.

This sample uses a different approach.

During our analysis, it launched the actual Chrome, Edge, and Firefox executables installed on the system. It started them in headless mode, disabled logging, and pointed each one at a temporary user-data directory.

In other words, it was not launching a fake browser. It was using legitimate browser binaries already trusted by the system.

The point is to work through a browser process that can access its own protected data rather than trying to defeat those protections from the outside.

Afterward, the malware issued commands to delete the temporary browser directories it had created.

The protection has not necessarily been broken. It has been approached through software that is already allowed to use it.

That is an important distinction, because browser-level encryption makes credential theft harder, but it cannot make running an unknown executable safe.

The delivery address can come from a social media profile

Vidar has a well-documented habit of using what researchers call **dead-drop resolvers**.

Instead of relying only on a command-and-control address permanently embedded in the malware, Vidar variants can retrieve the current destination from attacker-controlled profiles hosted on legitimate services such as Telegram and Steam.

This makes the infrastructure easier to rotate: operators can update a profile instead of rebuilding and redistributing the malware.

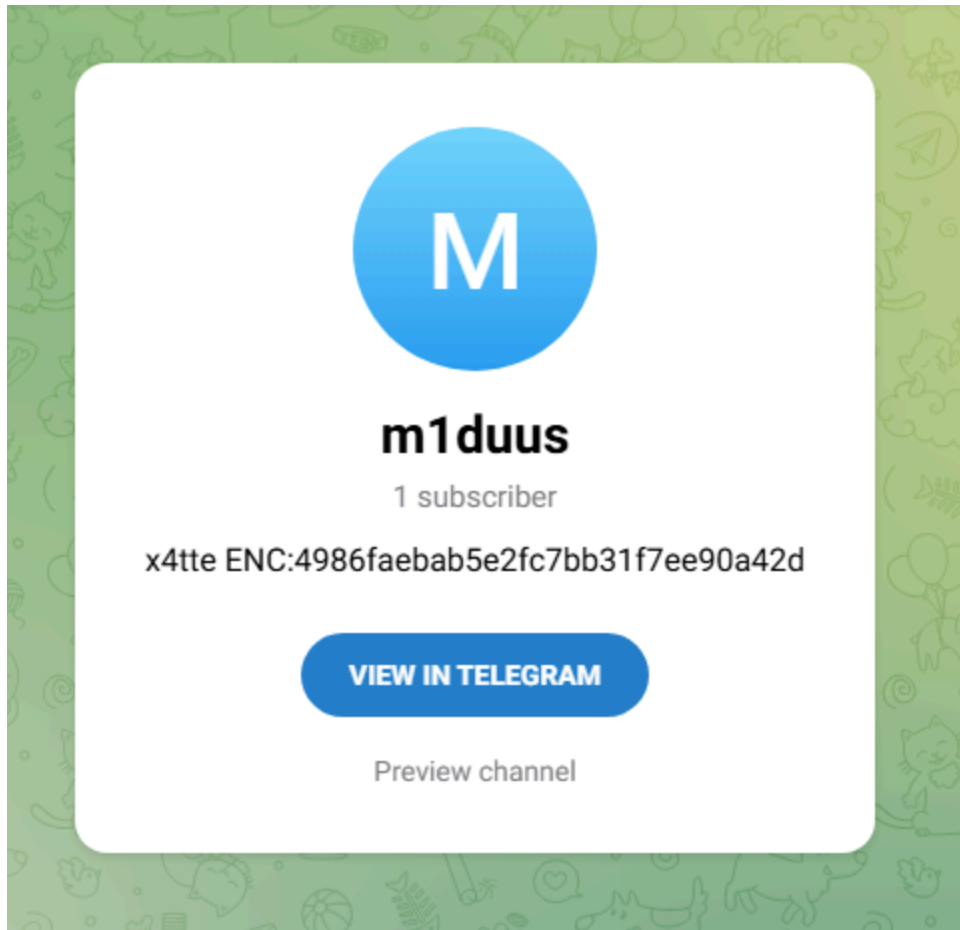
The activity we observed is consistent with that pattern.

The sample contained profile URLs for Telegram, Pinterest, and Steam Community, and network connections to all three services were observed during analysis.

It also communicated with attacker infrastructure. Most notably, it sent multipart POST requests to `ses.1001gacor.org`.

The sample also established a TLS connection to `ket.sm188daftar.mom`.

The important point is that traffic to a legitimate service such as Telegram, Pinterest, or Steam can blend in with ordinary network activity. Blocking one malicious server is also less useful when the malware has another place it can check for updated infrastructure.



The Telegram profile used by the malware

Indicators of compromise (IOCs)

Distribution sites

gta6demo[.]asia
gta6demo[.]eu
gta6demo[.]us
rockstar-gta-6[.]com

File hash (SHA-256)

a8f19d598e6a49d8510d73d41fc445246755ed321c2f76985a463a9fef537eb0
(gta6_installer.exe)

Dead-drop resolver URLs

telegram[.]me/m1duus
t[.]me/m1duus

pinterest[.]com/mlduus

steamcommunity[.]com/profiles/76561198657426610

Network infrastructure observed in this sample

ses.1001gacor[.]org

ket.sm188daftar[.]mom

Additional Vidar infrastructure

ket.1001gacor[.]org

ljr.1001gacor[.]org

nhg.1001gacor[.]org

bob.1001gacor[.]org

kra.1001gacor[.]org

brr.1001gacor[.]org

sto.1001gacor[.]org

rex.1001gacor[.]org

bib.1001gacor[.]org

ges.1001gacor[.]org

tax.11gokil[.]org

sii.11gokil[.]org

zaf.11gokil[.]org

dez.11gokil[.]org

tax.sm188dnsx[.]top

sii.sm188dnsx[.]top

zaf.sm188dnsx[.]top

2 0 2 6

CNET

**EDITORS'
CHOICE
AWARD**

“One of the best cybersecurity suites on the planet.”

According to CNET. [Read their review →](#)