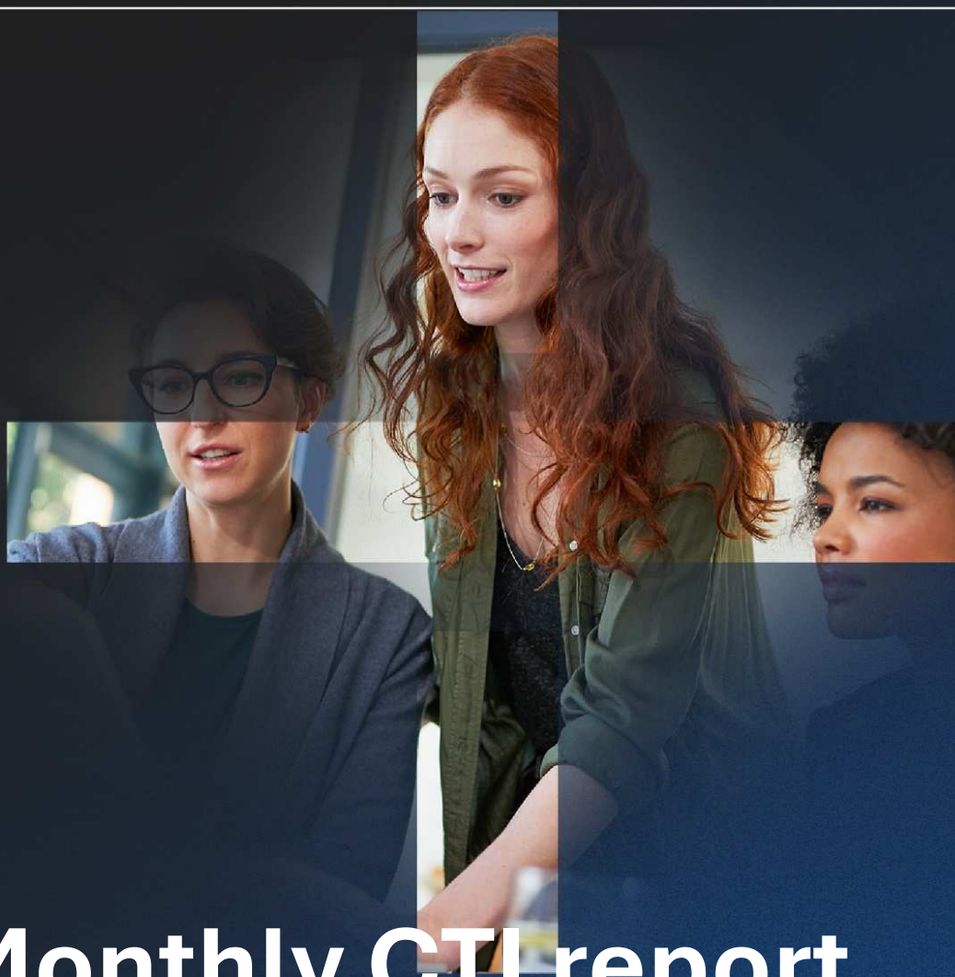
aDvens

For cyber, people & planet



Monthly CTI report

February 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, CERT aDvens offers an overview of emerging threats and current vulnerabilities to watch out for:

- Three new vulnerabilities, all of them with a public PoC, in addtion to those already identified.
- A technical analysis of a campaign targeting the gaming community, which involves the distribution of malware impersonating the mod Kiddion's Modest Menu for GTA V.

These topics aim to anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights three vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. Grandstream - CVE-2026-2329

A buffer overflow in the Grandstream GXP1600 series of VoIP phones allows a malicious actor to execute arbitrary code with root privileges.
This flaw can be exploited by sending specially crafted requests through the API endpoint /cgi-bin/api.values.get, which is accessible remotely and without authentication.

2.1.1. Type of vulnerability

- **CWE-121** : Stack-based Buffer Overflow

2.1.2. Risk

- Remote code execution

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted Products

- All models in the GXP1600 series (GXP1610, GXP1615, GXP1620, GXP1625, GXP1628, and GXP1630) versions prior to 1.0.7.81

2.1.5. Recommendations

Update all models in the GXP1600 series (GXP1610, GXP1615, GXP1620, GXP1625, GXP1628, and GXP1630) to version 1.0.7.81 or later.

Additional information is available in Grandstream's advisory.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. Keycloak - CVE-2026-1529

An improper verification of cryptographic signature of the invitation token in Keycloak, allows an attacker to successfully self-register and gain an unauthorized access to an organization.
This is made possible by modifying the fields "org_id" and "eml" inside the payload of a legitimate invitation token's JSON Web Token (JWT).

2.2.1. Type of vulnerability

→ **CWE-347** : Improper Verification of Cryptographic Signature

2.2.2. Risk

→ Security policy bypass

2.2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	None

2.2.4. Impacted Products

→ Keycloak versions prior to 26.5.3

2.2.5. Recommendations

Update Keycloak to version 26.5.3 or later.

Additional information is available in Keycloak's advisory.

2.2.6. Proof of concept

A proof of concept is available in open source.

2.3. Notepad++ - CVE-2026-25926

An unsafe search path vulnerability in Notepad++ allow an attacker to execute arbitrary code.
Notepad++ does not specify the absolute path to the binary "explorer.exe" when launching the file explorer. An attacker with local access could force the use of a malicious version of this binary, potentially leading to code execution.

2.3.1. Type of vulnerability

→ **CWE-426** : Untrusted Search Path

2.3.2. Risk

→ Remote code execution

2.3.3. Severity (base score CVSS 3.1)

Attack vector	Local	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	Required	Impact on availability	High

2.3.4. Impacted Products

→ Notepad++ versions prior to 8.9.2

2.3.5. Recommendations

Update Notepad++ to version 8.9.2 or later.

Additional information is available in Notepad++'s advisory.

2.3.6. Proof of concept

A proof of concept is available in open source.

3. THE GAMING COMMUNITY TARGETED: THE CASE OF KIDDION'S MODEST MENU

3.1. Introduction

Over the past few months, Advens' CERT has observed a significant increase in the number of credential thefts via malware that mimic the name of video game add-ons. This campaign can lead to the theft of personal and sometimes even professional credentials.

Among the most targeted vectors are mods, add-ons, cheat menus and free skins, mainly distributed via community platforms with little control. The case of "Kiddion's Modest Menu", a tool sought after by players looking to modify Grand Theft Auto V, perfectly illustrates this trend.

Although the initial project is regularly imitated and misappropriated, many unofficial sites now offer modified versions of the mod containing malicious payloads. Cybercriminals exploit a favourable context: strong user appeal, lack of source verification, trust in gaming communities and the difficulty of obtaining "official" versions. This report aims to provide an overview of the techniques observed, the malware identified and the recommendations that can be applied in this context.

3.2. Video games: an environment conducive to abuse

Gaming communities provide an ideal environment for malware distribution campaigns.

Unlike other communities, the gaming world encourages the creation of unofficial modifications. However, as these mods are considered illegal by game publishers, they do not always have reliable or verified sources. This situation facilitates the infiltration of malware, which can easily masquerade as simple modifications.

In addition, a significant proportion of gamers are teenagers and young adults, a highly connected audience that is sometimes less aware of cybersecurity risks. They are more likely to quickly download files without thorough verification.

Finally, fierce competition and frustration over performance (defeat, rankings, rare items that can be difficult to obtain) can make some players more impulsive. This impulsiveness increases the likelihood of clicking on links promising cheats, free skin generators or hacks that supposedly improve performance.

In 2025, the company Flare led an investigation on infostealer compromises and found that 41% of the identified compromises came from video game linked software, with Grand Theft Auto the most targeted game.

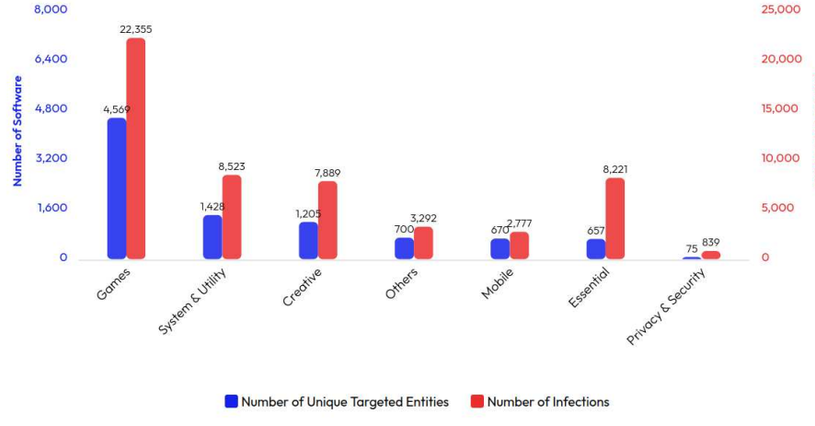


Figure 1. Types of software targeted by infostealers (source flare.io)

3.3. Kiddion's Mod Menu

Kiddion's Modest Menu, also named Kiddion's Mod Menu, is an external cheat menu for GTA V designed to add additional features such as money generation, vehicle spawning, stat modification and protection against certain actions by other players. Unlike many mods, this program does not inject code directly into the game, but works separately by modifying values from the outside (indirect memory read/write). It is available for free but does not have an official website.

The only source considered legitimate seems to be the UnknownCheats forum, where the mod's developer, Kiddion, updated it periodically. However, in June 2025, he announced that maintenance of the cheat would be discontinued.

Figure 2. Kiddion's post confirming the end of maintenance

Despite the end of these updates, the cheat remains extremely popular.

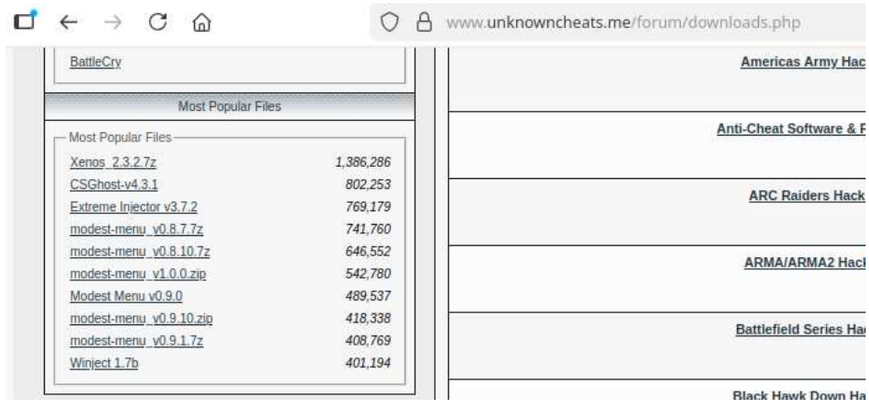


Figure 3. Most popular software on UnknownCheats

Due to this popularity, the menu is subject to numerous malicious copies distributed via third-party platforms.

3.3.1. Social engineering techniques observed

Many different methods are used to spread malicious versions of the software.

Fake official websites

As explained above, Kiddion's Mod Menu does not have an official distribution site. However, a Google search brings up numerous sites posing as the official site:

- kiddions[.]menu
- kiddionsmodmenu[.]com
- kiddion[.]org
- kiddions[.]com[.]de

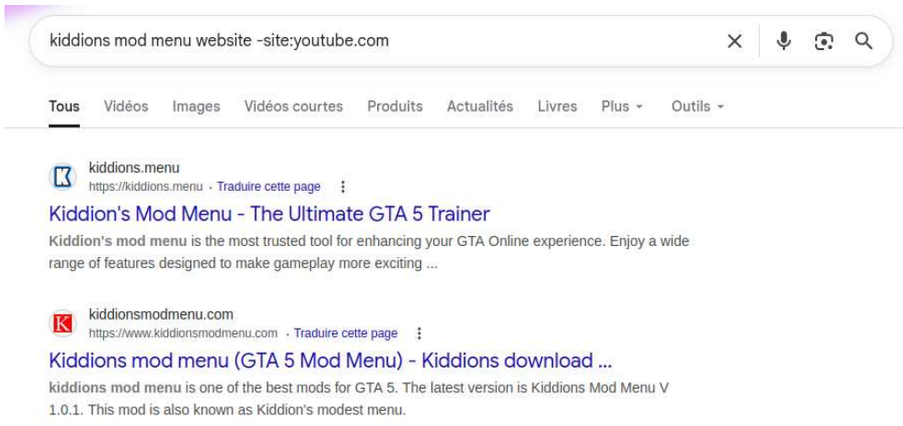


Figure 4. Google search Kiddion's Mod Menu

Improved versions

So-called "exclusive" versions, unofficial patches or modified forks are offered by third parties. These are usually distributed via forums, Discord servers or alternative communities. These versions often promise additional features, optimisations or compatibility with the latest game updates.

These incentives prove particularly effective in cheating communities, where competition between legitimate and modified tools confuses users.

Compromised YouTube accounts

Another method used to distribute these mods is to use compromised YouTube accounts.

Indeed, YouTube has long been abused for sharing malware. Since November 2025, compromised YouTube accounts have been used to distribute video tutorials for installing cheat software, such as [.orange]#Kiddion's Mod Menu, or cosmetic items, such as Fortnite skins. Some of the compromised accounts have not been active for several years, and the malicious posts often have no connection to the videos posted before the compromise.

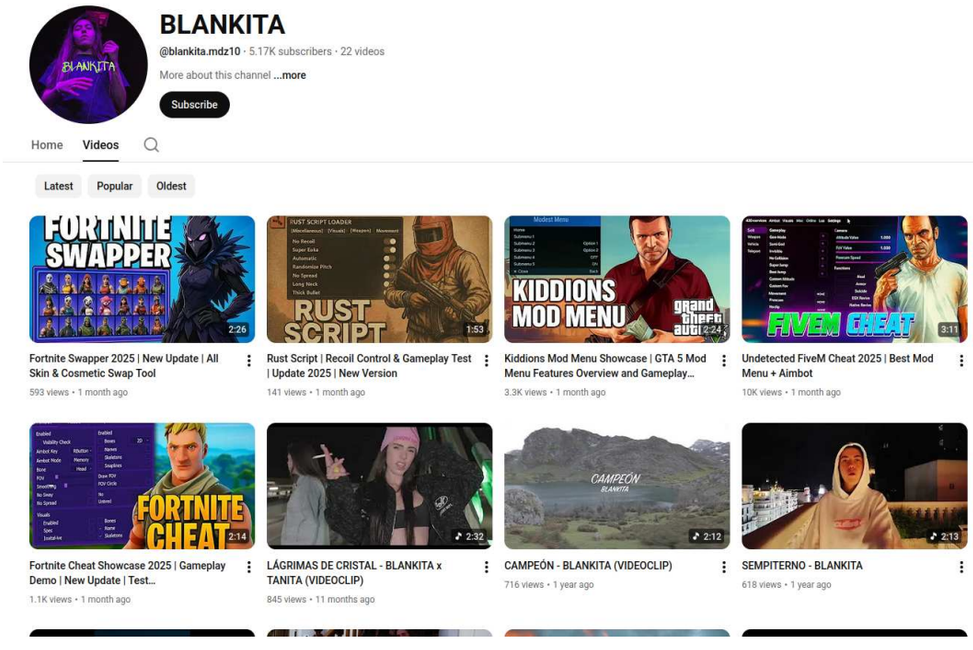


Figure 5. Compromised YouTube account

The videos are all created in the same way, with an AI-generated image as the cover. They begin with an explanation of how to install the program via Mediafire, followed by a quick demonstration of the mod in action in the game. The download links are

posted in the description of the post along with the archive password (often *gtamod*, *2024*, *gta5*, etc.). They are often published in batches of videos within a very short period of time.

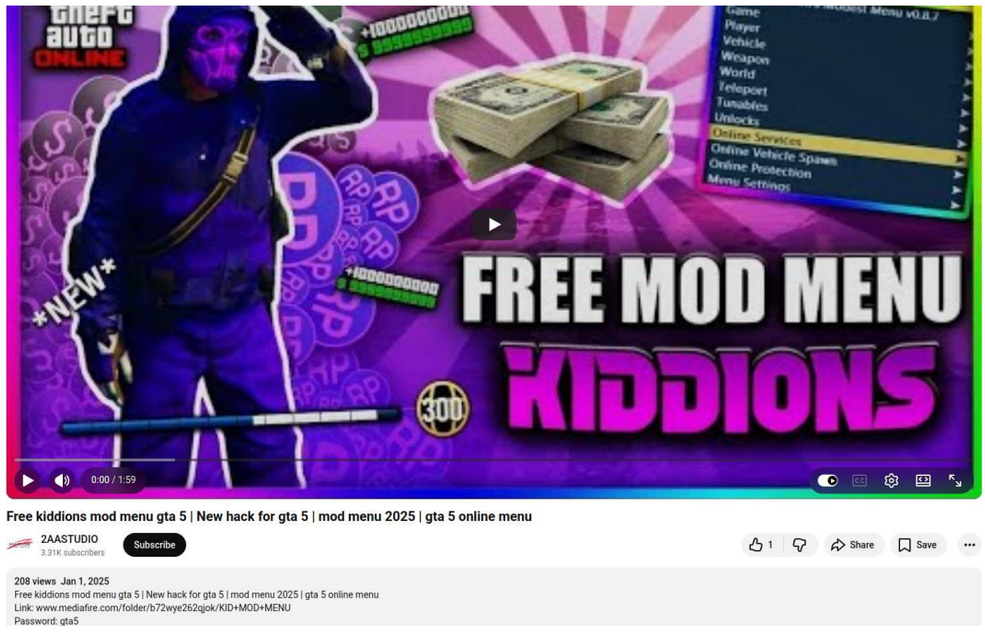


Figure 6. Example video Kiddion's Mod Menu

3.3.2. Analysis of a sample

A sample, available on the compromised channel "Voice of the Quran" (hxxps://www.youtube[.]com/watch?v=ZB2QgR5HBIw), was selected for analysis. The archive *Kiddion's Modest Menu.zip* is downloaded from mediafire[.]com. This file is 106 MB in size, approximately 90 MB larger than the "legitimate" file available on UnknownCheats. The archive is extracted using the password *gtamod*.

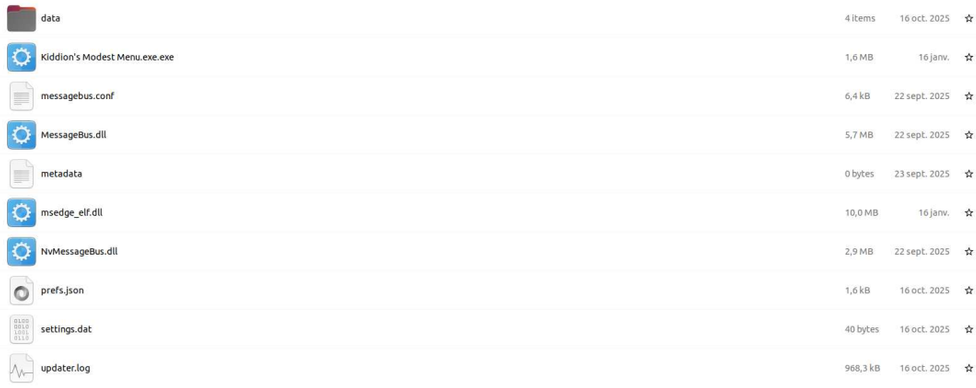


Figure 7. Extraction of the Kiddion's Modest Menu.zip archive

The *data\Log* folder contains a binary file named JPcd56xErJkLadWe, which is 104.9 MB in size. The role of this binary file could not be determined during analysis.

In the tutorial, the user is prompted to run the file named Kiddion's Modest Menu.exe.

Kiddion's Modest Menu.exe.exe

- md5: e31770026101eaccb1b5de7cffd52033
- sha1 235beed3a3c2ecb6415eff789d2f4deb2cd28c3b
- sha256: 232fa5792839dc677b0211b3694954e9660b174aa0f9bedcab772ac1e86d3843
- size: 1.56 MB

This file is signed by Microsoft. It is the legitimate binary identity_helper.exe that has been renamed. This binary has already been observed in *DLL SideLoading* campaigns. By placing a file named msedge_elf.dll in the same folder, it will be executed by the legitimate binary in the context of a Microsoft-signed process, bypassing most defences based on the reputation of the parent process.

msedge_elf.dll

- md5: ea355db3afdbe9b85efcaed57261300f
- sha1: 46ddbd992fcd977adda890fff8e7fde878799667
- sha256: e941d70f7367e1ee3e71850335febf9a23fd57aa98bbcdc1e0c0b0ee45406ccd
- size: 9.99 MB

This malicious DLL (whose internal PE name is Crypt.dll) is written in Go.

```
Go build ID: "ckBPoM7cfgUd759qqRF0/JJpD8eX_Ss7UoLIQavjc/lcJUpWeNz27IEffK9fvN/Py834-zicsgsx6EshZcT"
```

Figure 8. Go build ID

Before performing malicious actions, the DLL performs several tasks to hinder analysis:

- A set of checks with the C2 server. Six commands are checked (*stageOneAbort*, *stageTwoAbort*, *immediateAbort*, *emergencyProcedureAlpha/Beta/Gamma*). If any of them are active, the malware stops.
- Floating calculations related to space (altitude, velocity, thrust, inclination) are performed. These calculations could be linked to the functioning of the mod menu.

Furthermore, all main.* functions have names composed of concatenated English words (up to 1,350 characters), making PCLNTAB Go unreadable without manual processing.

```
main.main
main.Invitation
main.committeedisclosureprogrammingpermanentsubdivisionconversationinternationalnorwegiancontractorsfor
main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectionabsc
main.main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectic
main.main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectic
monyvietnamesegentlemanpartnershipsrecordersannouncementsvbulletinmarijuanapsychologycigarettesorganizi
main.main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectic
ettesorganizingacceptingcelebraterecruitingcompositereferencesdangerousinstitutionalreasonablyvalentine
tlemanpartnershipsrecordersannouncementsvbulletinmarijuanapsychologycigarettesorganizingacceptingcelebr
.main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectionabs
main.main.housewarespredictedsustainabilitycumulativepermissionsdepartureadvertiserscombinationdetectic
```

Figure 9. Function obfuscation

The payload is embedded directly in the .rdata section of the DLL via the Go *//go:embed* mechanism, under the file name *confirmed* (596 KB).

The decryption is performed in three successive in-memory passes:

- 0x7D (125) is added to each byte, modulo 256
- The buffer is inverted
- 0x7D (125) is added to even bytes and taken away from odd bytes, modulo 256.

This DLL, loaded directly into memory by the Go loader, was extracted and analysed.

```
29fa12c42  0fb61401          movzx   edx, byte [rcx+rax]
29fa12c46  83c27d            add     edx, 0x7d
29fa12c49  881408            mov     byte [rax+rcx], dl
29fa12c4c  48ffc1            inc     rcx

29fa12c4f  4839cb            cmp     rbx, rcx
29fa12c52  7fee              jg      0x29fa12c42

29fa12c54  48898424f0000100  mov     qword [rsp+0x100f0], rax
29fa12c5c  488d53ff          lea     rdx, [rbx-0x1]
29fa12c60  31c9              xor     ecx, ecx
29fa12c62  31db              xor     ebx, ebx
29fa12c64  31f6              xor     esi, esi
29fa12c66  eb0b              jmp     0x29fa12c73

29fa12c68  45884c08ff        mov     byte [r8+rcx-0x1], r9b
29fa12c6d  48ffca            dec     rdx
29fa12c70  4c89c6            mov     rsi, r8

29fa12c73  4885d2            test    rdx, rdx
29fa12c76  7c5c              jl      0x29fa12cd4

29fa12c78  4c8d4601          lea     r8, [rsi+0x1]
29fa12c7c  440fb60c02        movzx   r9d, byte [rdx+rax]
29fa12c81  4c39c3            cmp     rbx, r8
29fa12c84  73e2              jae     0x29fa12c68
```

Figure 10. Decryption routine

Malware extrait

- md5: 4126455cf7bd781bc0dcece1e9fd03ff
- sha1: 285b24835fc1be15ffa611d3546e846739a4b942
- sha256: f3e0fb836f4457c2c98383e26d504d7512436f8bc729a5f436a157ddf058fe07
- size: 596.07 KB

This Windows executable is not known in open source. It is detected by Sophos as the infostealer Vidar.

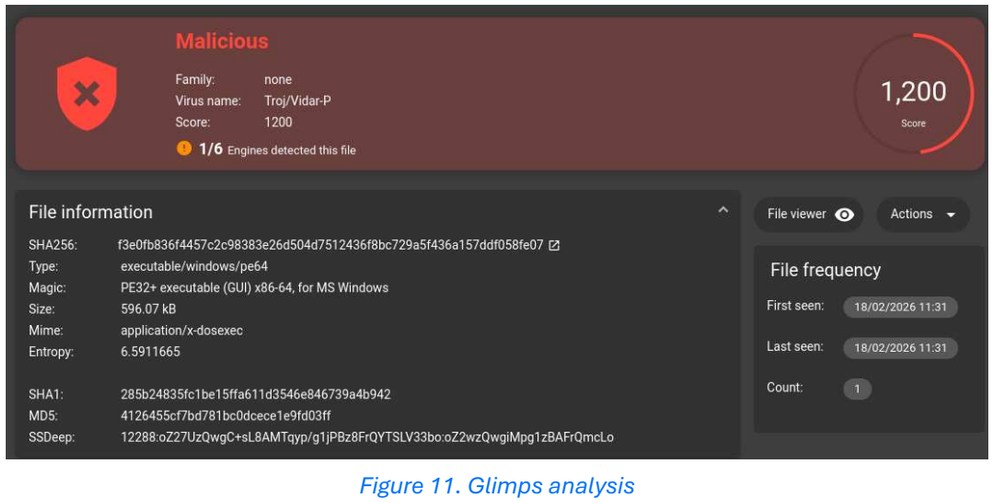


Figure 11. Glimps analysis

This malware seeks to steal information from the system by targeting:

- Browsers (Chrome, Firefox, Opera, Chromium, Edge) to extract passwords, cookies, history and web extensions
- Cryptocurrency wallets
- Files from the %DESKTOP%, %DOCUMENTS% and %DOWNLOADS% folders with the extensions .txt, .ps1, etc.

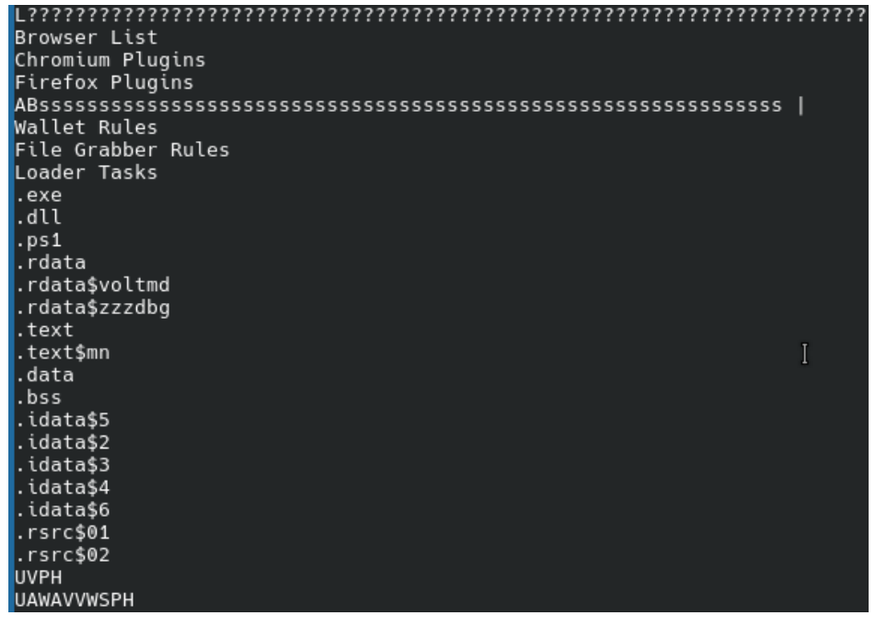


Figure 12. Extracted strings

By performing XOR operations on the still-obfuscated code, the domain amcommunity[.]com was extracted. This inactive domain was seen in an analysis of msedge_elf.dll.dll by the JoeSandbox platform. This malware is also identified as a Vidar infostealer.

3.4. Conclusion

The installation of infostealers or malware on users' personal machines poses a major threat to security of companies. This malicious software is capable of extracting sensitive information such as credentials, session cookies, authentication tokens and data stored in browsers.

When users log into their work accounts from an infected device, attackers can then usurp their identity, bypass authentication mechanisms and penetrate internal environments. This gateway between uncontrolled personal devices and work resources increases the risk of compromise, data leaks and even major incidents affecting entire information systems. The abuse of stolen accounts remains criminals primary source of compromise of company systems.

3.5. Recommendations

To reduce the risks associated with installing malware via video game mods on personal computers, several measures must be put in place:

- It is essential to raise awareness among users about the dangers associated with downloads from unverified sources and to encourage the use of official applications or recognised platforms.
- Organisations must promote a strict separation between personal and professional use, in particular by prohibiting access to professional accounts from unmanaged devices.
- Implementing solutions such as robust multi-factor authentication, authentication anomaly detection, and work environment isolation (VDI, secure browsers, managed devices) greatly limits the impact of a compromise.
- Maintaining a security solution on personal computers (up-to-date antivirus software, regular updates and good digital practices) helps to reduce the attack surface and prevent these infections.

3.6. Indicators of compromise

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	domain	amcommunity[.]com	Suspicious
TLP:CLEAR	domain	kiddions[.]menu	Malicious
TLP:CLEAR	domain	kiddionsmodmenu[.]com	Malicious
TLP:CLEAR	domain	kiddion[.]org	Malicious
TLP:CLEAR	domain	kiddions[.]com[.]de	Malicious
TLP:CLEAR	Archive	Kiddions Modest Menu.zip	Malicious
TLP:CLEAR	MD5	513967d5e4e4b6f1aedd5c6e0fb5b25c	Malicious
TLP:CLEAR	SHA-1	b47465d959207a18d568a5692acaedc502ea899d	Malicious
TLP:CLEAR	SHA-256	aac73a471e256d9c6bfae6fc2ae4dd90b0e352884a4485af16a3729dae4d325e	Malicious
TLP:CLEAR	PE File	Kiddion's Modest Menu.exe.exe	Malicious
TLP:CLEAR	MD5	e31770026101eaccb1b5de7cffd52033	Legitimate identity_helper.exe
TLP:CLEAR	SHA-1	235beed3a3c2ecb6415eff789d2f4deb2cd28c3b	Legitimate identity_helper.exe
TLP:CLEAR	SHA-256	232fa5792839dc677b0211b3694954e9660b174aa0f9bedcab772ac1e86d3843	Legitimate identity_helper.exe
TLP:CLEAR	PE File	msedge_elf.dll	Legitimate file name used for malicious purposes
TLP:CLEAR	MD5	ea355db3afdbe9b85efcaed57261300f	Malicious
TLP:CLEAR	SHA-1	46ddbd992fcd977adda890fff8e7fde878799667	Malicious
TLP:CLEAR	SHA-256	e941d70f7367e1ee3e71850335febf9a23fd57aa98bbcdc1e0c0b0ee45406ccd	Malicious
TLP:CLEAR	MD5	4126455cf7bd781bc0dcece1e9fd03ff	Vidar Malicious
TLP:CLEAR	SHA-1	285b24835fc1be15ffa611d3546e846739a4b942	Vidar Malicious
TLP:CLEAR	SHA-256	f3e0fb836f4457c2c98383e26d504d7512436f8bc729a5f436a157ddf058fe07	Vidar Malicious

4. SOURCES

Grandstream - CVE-2026-2329

- https://psirt.grandstream.com/

Keycloak - CVE-2026-1529

- https://www.keycloak.org/2026/02/keycloak-2653-released

Notepad++ - CVE-2026-25926

- https://community.notepad-plus-plus.org/topic/27412/notepad-v8-9-2-release

The gaming community targeted: the case of Kiddion's Modest Menu

- https://flare.io/learn/resources/cybercrime-favorite-target-gamers
- https://www.youtube.com/
- https://blog.checkpoint.com/security/how-threatcloud-ais-threat-emulation-engine-prevents-dll-sideloading-trojan-attacks/
- https://www.virustotal.com/
- https://www.joesandbox.com