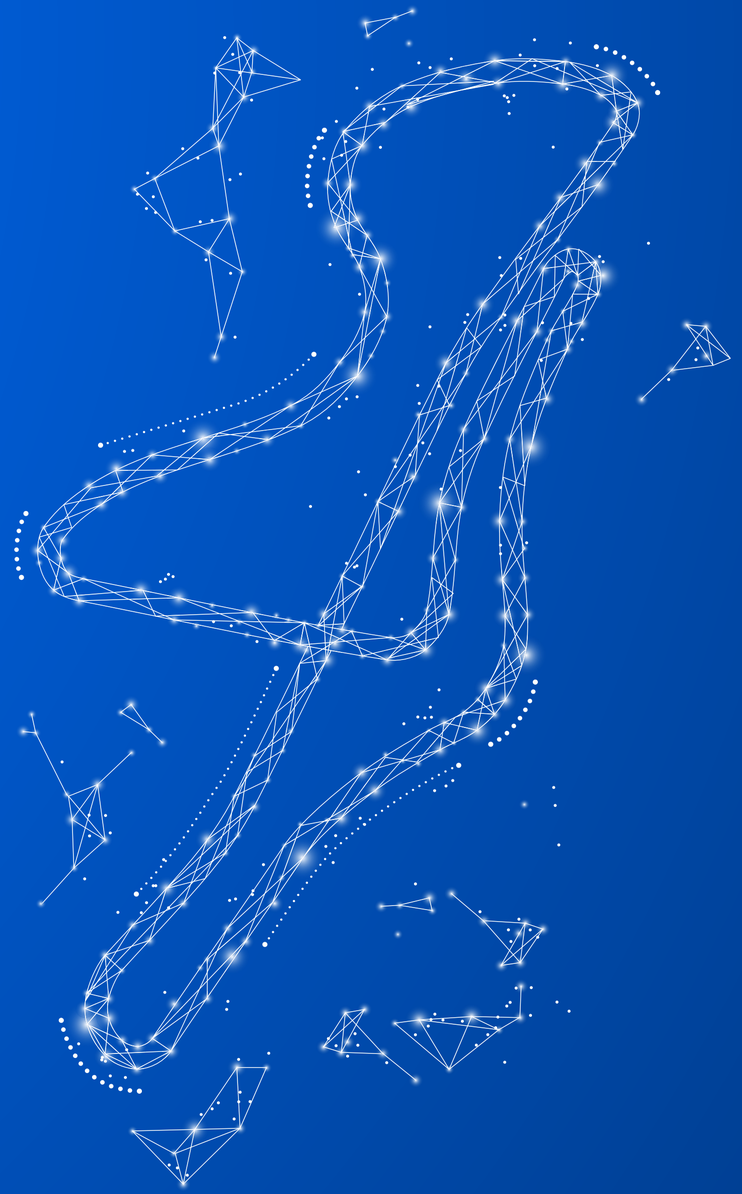
Bitdefender

Fan Threat Index

CYBERSECURITY GRAND PRIX



Bitdefender

Why motorsport?



While motosport teams and organizers invest heavily in protecting race telemetry, intellectual property, and trackside infrastructure, far less attention has been paid to the consumer threat landscape surrounding the sport itself.

A SEASONAL SCAM ECONOMY

Modern motorsport operates as a global digital ecosystem. Tickets are sold online through fragmented regional vendors, races are distributed through expensive streaming agreements, and merchandise sales are amplified by social media advertising and influencer campaigns. This combination creates ideal conditions for fraud operations.

The result is a seasonal scam economy that intensifies around race weekends, major announcements, and championship milestones.

HOW CYBERCRIMINALS EXPLOIT MOTORSPORT FANS

This chapter does not focus on attacks against motorsport teams themselves. Instead, it explores how cybercriminals exploit motorsport fans through scams, counterfeit ecosystems, illegal streaming infrastructure, and social engineering.

Bitdefender

Motorsport creates ideal conditions for fraud

Urgency is one of the strongest psychological triggers in scams. Motorsport naturally creates urgency every race weekend.



Bitdefender

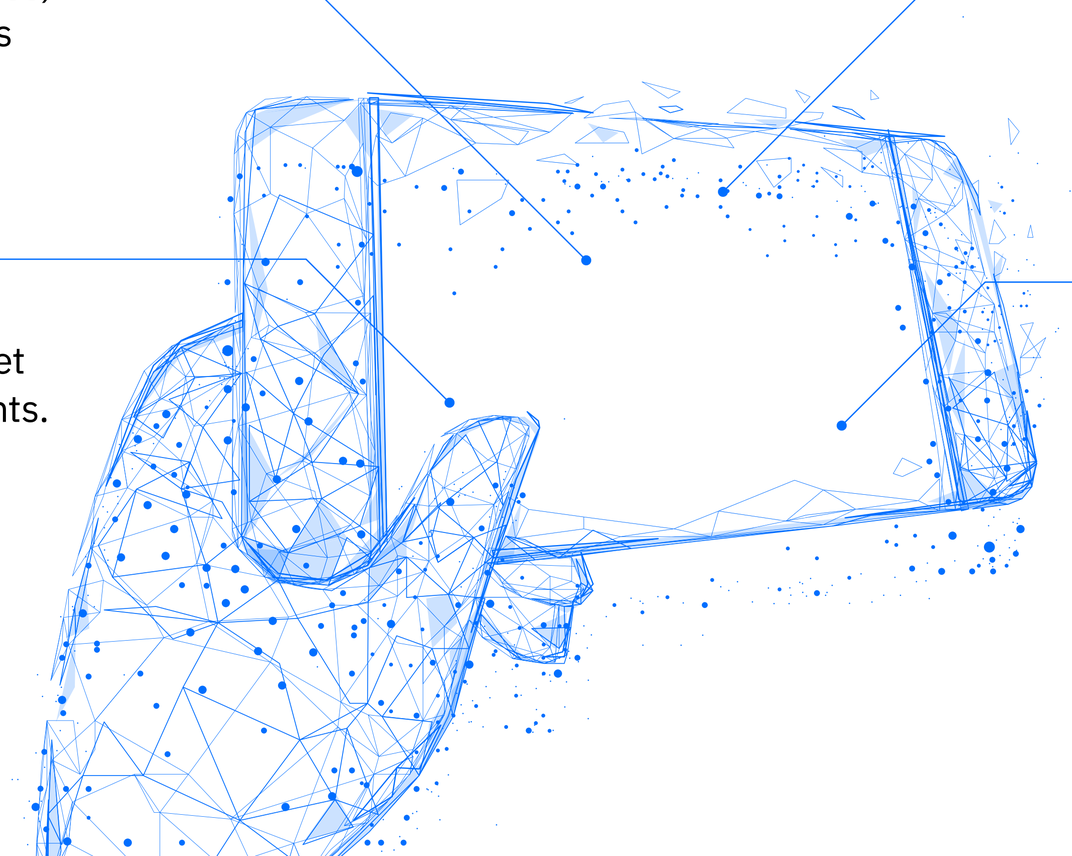
Main scam categories observed

COUNTERFEIT MERCHANDISE

Fake team apparel, accessories, jackets, caps, and collectibles promoted via social media advertising.

TICKET SCAMS

Fake resale websites and fraudulent “last chance” ticket offers targeting sold-out events.



ILLEGAL STREAMING ECOSYSTEMS

Fake streaming portals, IPTV services, malicious APK distribution, and aggressive ad monetization.

SOCIAL ENGINEERING & IMPERSONATION

Fake giveaways, VIP access offers, paddock pass scams, and impersonation of teams or sponsors.

Bitdefender

Threat **timeline** around race weekends

Scam activity follows predictable cycles

BEFORE RACES

→ ticket scams spike

→ fake merchandise ads increase

→ phishing and giveaways intensify

DURING RACES

→ illegal streaming campaigns surge

→ APK distribution increases

→ Discord and Telegram activity spikes

AFTER RACES

→ replay scams

→ highlight clip scams

→ survey and giveaway abuse

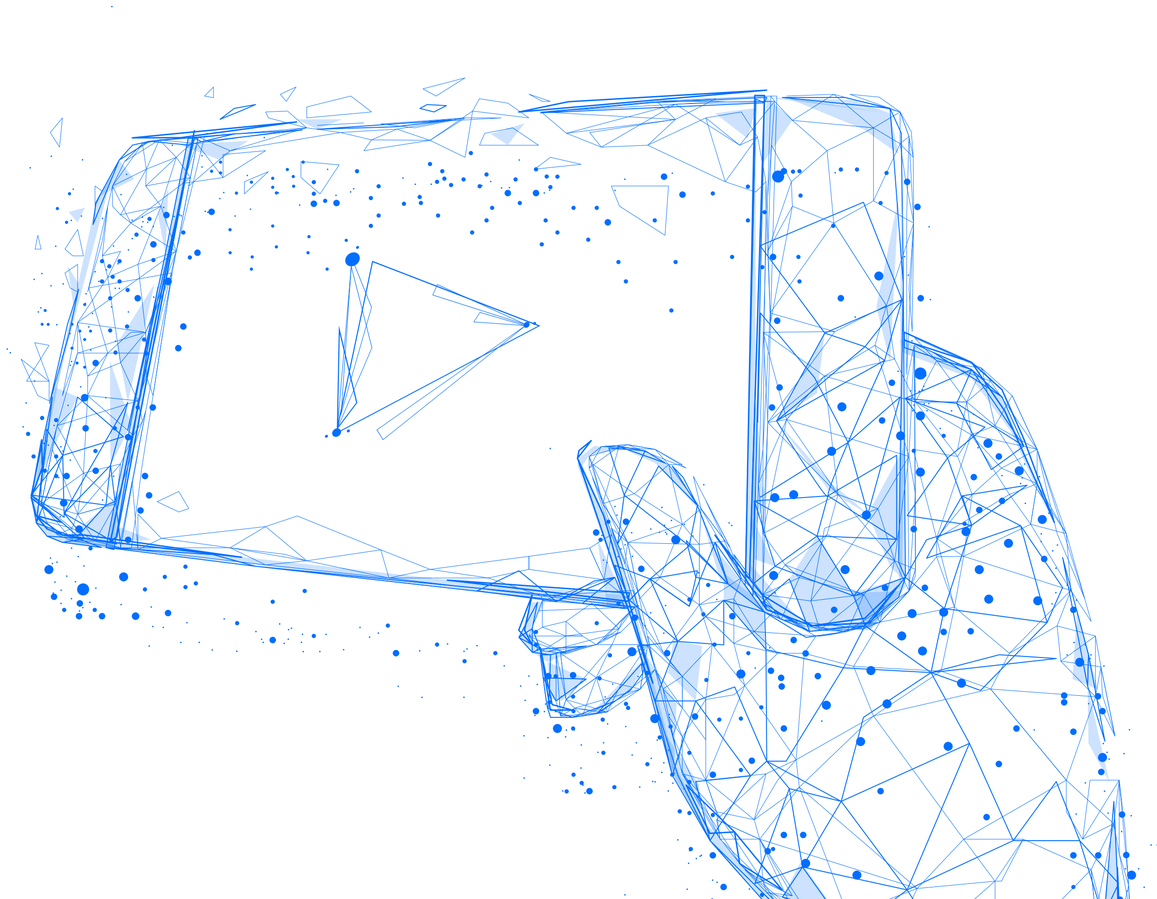


Bitdefender

Free motorsport streams often act as **scam funnels**

Research identified multiple websites claiming to offer free motorsport broadcasts while redirecting users toward:

- → fake subscriptions
- → VPN upsells
- → aggressive advertising
- → adult content
- → Telegram channels
- → APK downloads



> Users attempting to access unauthorized streams often have limited recourse after being defrauded, since the service itself operates outside legal channels.

Bitdefender

Common behavioral patterns

SOCIAL AMPLIFICATION

Streaming links heavily promoted through:

→ Facebook groups

→ Reddit discussions

→ Discord watch parties

→ Telegram coordination channels

MONETIZATION-FIRST BEHAVIOR

Many websites appear designed primarily to:

→ collect payments

→ force ad interactions

→ redirect users

→ push mobile apps

In many cases, the actual motorsport stream appears secondary to monetization.

DISPOSABLE INFRASTRUCTURE

Domains frequently appear shortly before race weekends and disappear rapidly afterward.

Bitdefender

Android streaming applications

Sideloaded streaming apps increase exposure.
Applications such as **Playfy TV** and **Cricfy TV** advertise free access to motorsport broadcasts but require users to manually install APK files outside official app stores.

Observed behaviors include:

→ excessive advertising

→ forced redirects

→ aggressive popups

→ affiliate abuse

→ installation prompts for unrelated applications



The piracy ecosystem increasingly overlaps with mobile ad abuse and potentially malicious distribution chains.

Bitdefender

Android streaming boxes

BADBOX 2.0: a massive bot built around streaming devices. The BADBOX botnet is a significant cybercriminal operation that targets Android streaming boxes. This botnet is known for compromising devices before they reach consumers, embedding malware that allows for various illegal activities.

KEY FEATURES OF BADBOX 2:

→ Type of malware: Backdoor, Bot, Proxy

→ Affected operating systems: Android

→ Device types: Mobile phones, tablets, smart TVs

→ Impact Level: High



> WHAT WE INVESTIGATE > CYBER > CYBER ALERTS > 2025

FBI

What We Investigate

Terrorism | Counterintelligence and Espionage | Cyber | Public Corruption | Civil Rights | Transnational Organized Crime

News | Partners | Cyber Alerts | SEC Reporting Requirements | Most Wanted

Public Service Announcement

X.com

June 5, 2025

Home Internet Connected Devices Facilitate Crimina

Alert Number: I-060525-PSA

Questions regarding this PSA should be directed to your local FBI field office.

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement to warn the public about cyber c
Internet of Things (IoT)[1] devices connected to home networks to conduct criminal activity using the BADBOX 2.0 botne
gain unauthorized access to home networks through compromised IoT devices, such as TV streaming devices, digital p
vehicle infotainment systems, digital picture frames and other products. Most of the infected devices were manufacture
criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to
infecting the device as it downloads required applications that contain backdoors, usually during the set-up process.[3] C
compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of th
and residential proxy services[4] known to be used for malicious activity.

What is BADBOX 2.0 Botnet?

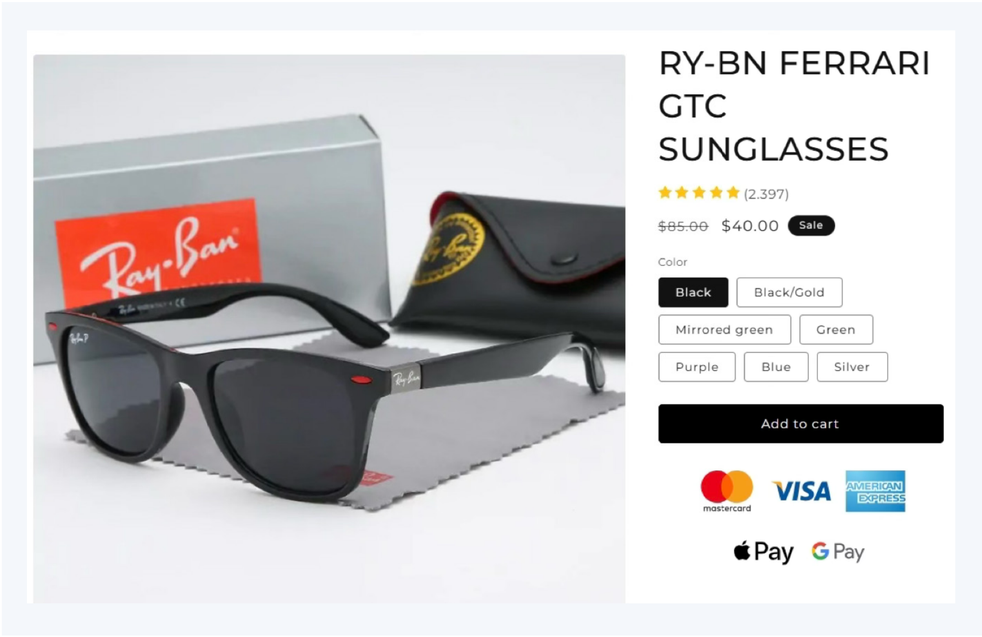
BADBOX 2.0 was discovered after the original BADBOX campaign was disrupted in 2024. BADBOX was identified in 2
consisted of Android operating system devices that were compromised with backdoor malware prior to purchase. BADI
compromising devices prior to purchase, can also infect devices by requiring the download of malicious apps from unof

The BADBOX 2.0 botnet consists of millions of infected devices and maintains numerous backdoors to proxy services f
actors exploit by either selling or providing free access to compromised home networks to be used for various criminal

Bitdefender

Counterfeit merchandise campaigns

Fake motosport shops aggressively advertise on social media. Researchers identified campaigns promoting heavily discounted motorsport branded merchandise through Meta advertising infrastructure.



OBSERVED CHARACTERISTICS:

→ “80% OFF” urgency messaging

→ cloned storefront designs

→ unrealistic pricing

→ geographically targeted advertising

→ newly established domains

→ poor trust reputation indicators

Bitdefender

The “80% OFF” pattern

Recycled scam infrastructure across major sports events

The campaign structure closely resembles previously documented scam campaigns observed during other high-profile sporting events, including the Olympics.

NOTABLE SIMILARITIES:

→ identical discount language

→ cloned ecommerce layouts

→ urgency-focused copywriting

→ broad audience targeting

→ short-lived advertising bursts



Bitdefender

Advertising intelligence findings

Indicators of organized counterfeit operations

Campaign characteristics:

→ multi-country targeting

→ sustained ad spend

→ multiple ad variants

→ audience segmentation

→ polished storefront presentation

> One identified ad cluster operated for seven days and targeted United Kingdom, Australia and Ireland.
>
> This behavior resembles professional ecommerce advertising operations more than traditional low-effort scam pages.

Bitdefender

Discord and Telegram coordination

Community platforms enable resilient distribution

Illegal motorsport streaming communities increasingly rely on:

→ Discord servers

→ Telegram channels

→ backup invite systems

OBSERVED BEHAVIOR:

→ stream references removed after races

→ migration to backup servers

→ rapid link rotation

→ disclaimers denying direct hosting



These communities operate similarly to resilient content distribution networks.

Bitdefender

The rise of ClickFix-style attacks

ClickFix attacks rely on social engineering instead of software exploits.

Victims are instructed to:

→ “fix” playback problems

→ “enable streaming access”

→ “verify browser security”

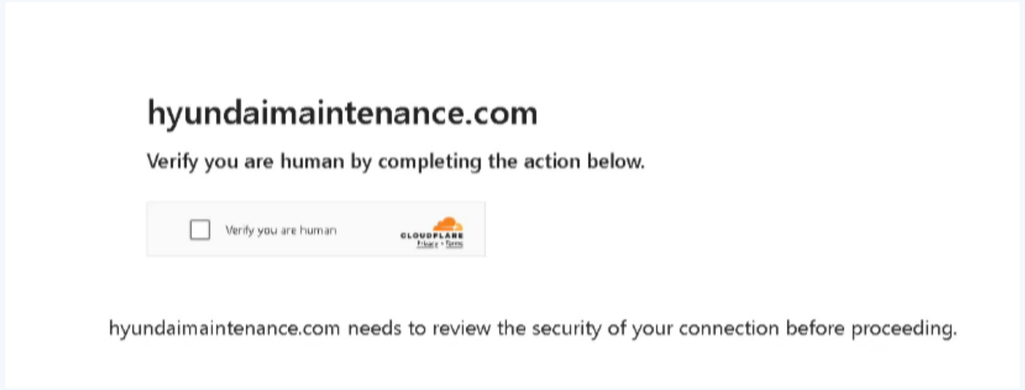
→ “update codecs”

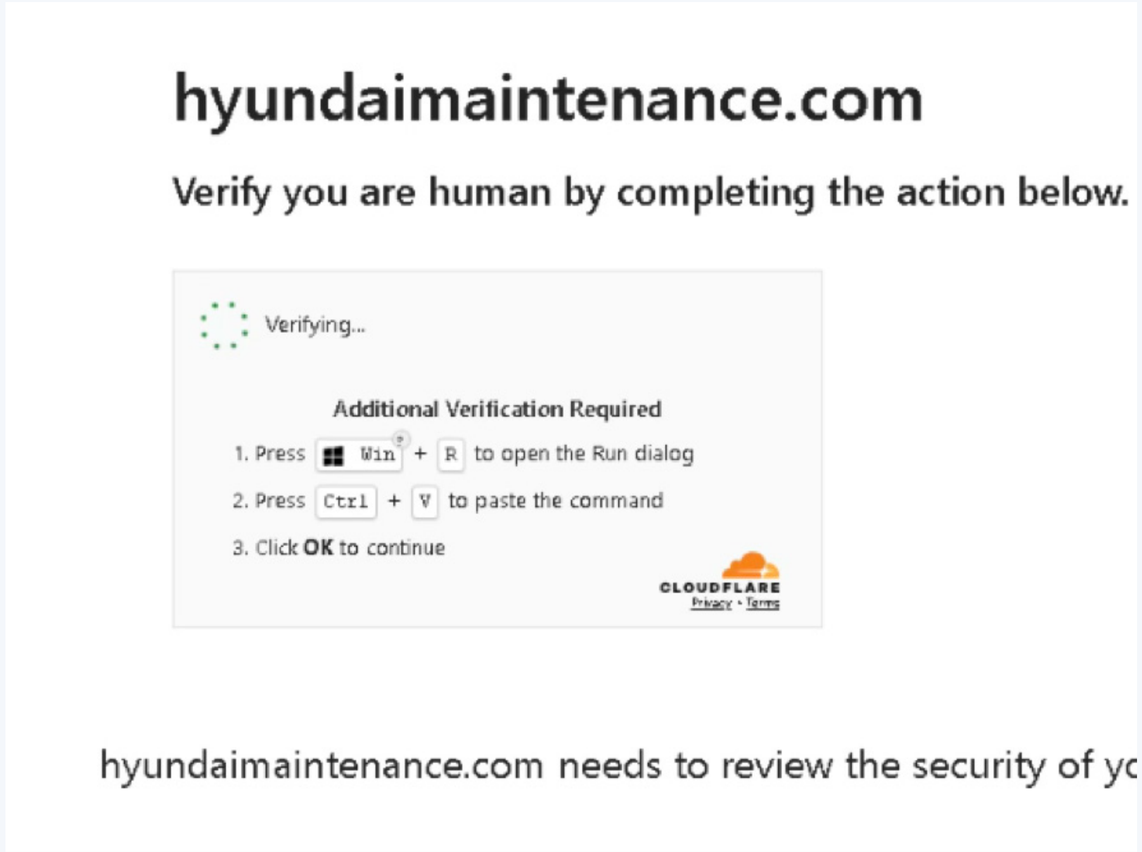
→ “repair buffering issues”

The objective is to convince users to execute malicious commands or install malware themselves.

Bitdefender

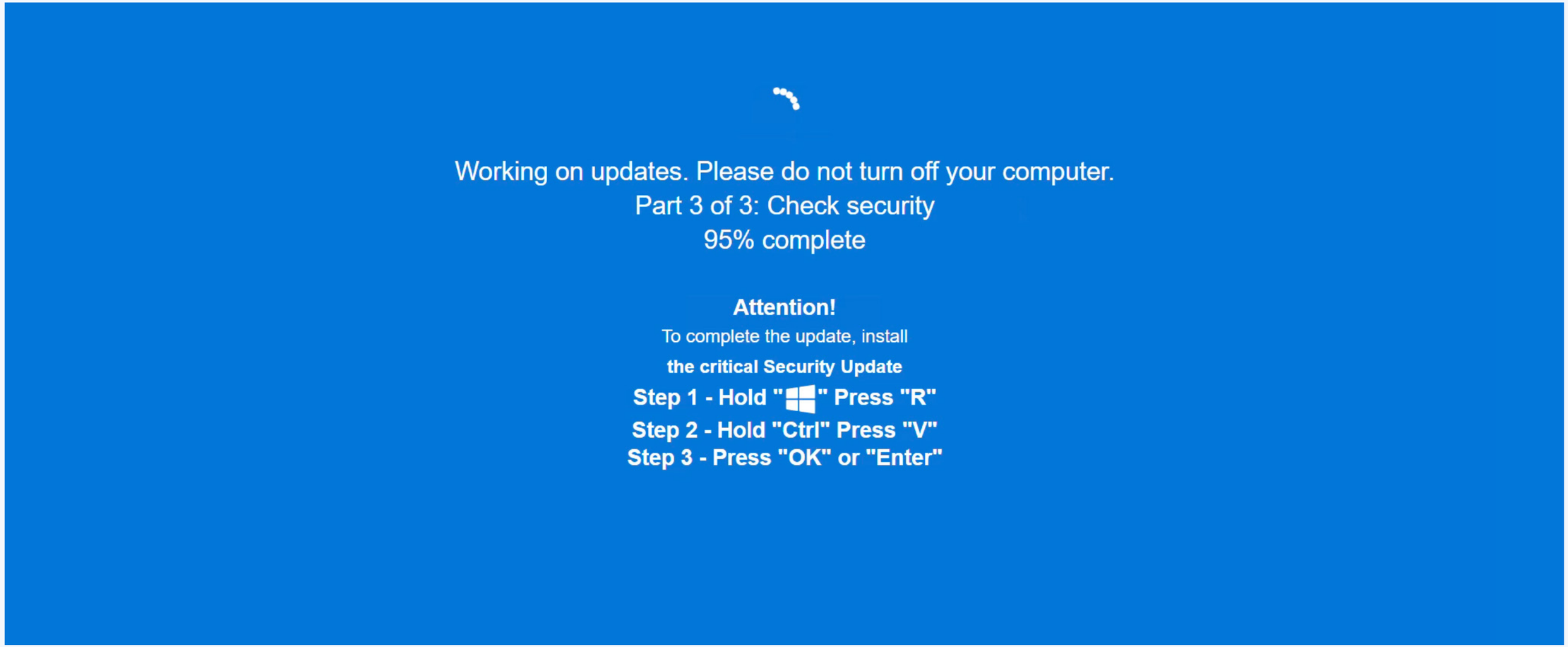
What ClickFix looks like





Bitdefender

What ClickFix looks like



Bitdefender

How ClickFix works

A typical workflow starts with the user searching for free video streaming resources.

However, when the victim reaches the desired page, they are instructed to:

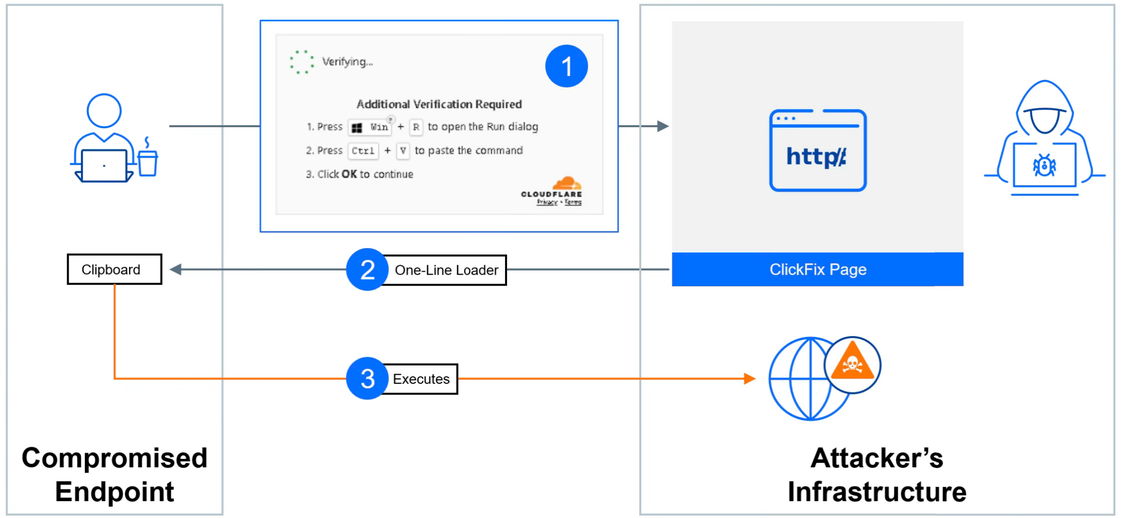
→ copy PowerShell commands

→ paste terminal commands

→ install “required updates”

→ execute downloaded scripts

Malware executes locally, via applications that live inside the operating system.



1 **Deception (CAPTCHA):** The user is presented with a fake, legitimate-looking error or verification screen.

2 **Clipboard Copy:** Malicious JavaScript injects a one-line "living-off-the-land" command directly into the user's clipboard.

3 **Execution:** The site instructs the user to open the Run dialog, paste the content, and hit enter, tricking the user into manually executing the payload.

Bitdefender

Enter the infostealer

Infostealers are optimized for silent credential theft

COMMON MALWARE FAMILIES INCLUDE:

→ Lumma

→ RedLine

→ Vidar

→ StealC

→ Raccoon

PRIMARY TARGETS:

→ browser passwords

→ session cookies

→ saved payment cards

→ crypto wallets

→ VPN credentials

→ email access

Bitdefender

Session cookies are now a primary target

Attackers increasingly bypass passwords entirely.

MODERN INFOSTEALERS FOCUS HEAVILY ON:

→ authenticated browser sessions

→ stored tokens

→ persistent cookies

POTENTIAL IMPACT:

→ account takeover

→ MFA bypass in some scenarios

→ persistent access to services

Bitdefender

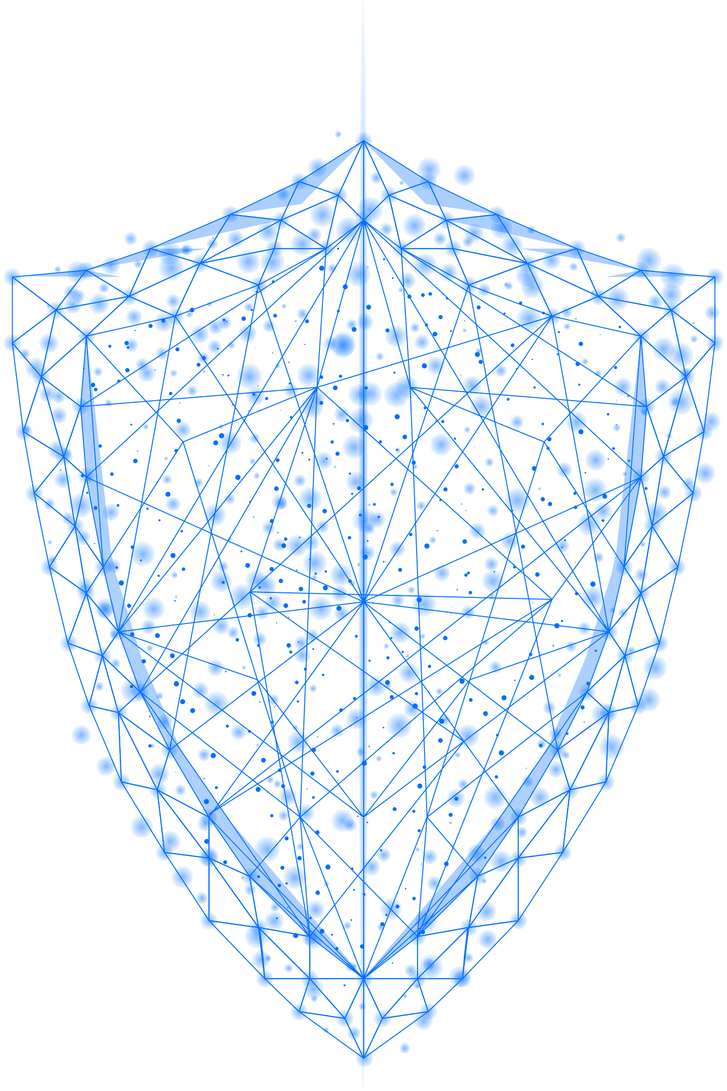
How Bitdefender can help

Our protection layers address scams at multiple control points. Online Threat Prevention inspects and blocks malicious URLs and exploit attempts at the network level, regardless of how the link was delivered - email, SMS, messaging apps or social media.

Anti-Phishing and Anti-Fraud engines analyze web page structure, domain age, impersonation patterns and behavioral indicators to stop credential harvesting and payment fraud.

Scamio provides AI-assisted scam validation, allowing users to submit suspicious messages, screenshots or links and receive rapid, intelligence-backed risk assessments.

On mobile, Call Blocking and scam detection features flag or suppress known fraudulent numbers, while Web Protection monitors browsing sessions to prevent redirection to malicious domains.



Bitdefender is a **Global Leader in Cybersecurity**

Protecting millions of consumer and business environments since 2001

We take pride in our Telco-oriented solutions that include Value-Added Services, Core Network Security and Management & Intelligence Platforms, as well as the partnerships we established with some of the biggest Service Providers in the world.

HEADQUARTERS
Bucharest, Romania
Fort Lauderdale, Florida

WORLDWIDE OFFICES
Europe & US HQs
17 regional offices across US, Europe, Asia and Australia

PARTNERS
35,000+ qualified partners and resellers
Distributed through partners in **170** countries

CONTINUED INNOVATION
540+ patents

EMPLOYEES
2100+
More than half of Bitdefender's employees are security researchers and engineers

