Global Leader
In Cybersecurity

Bitdefender®

Deepfakes Unmasked: Technical Landscape of Modern Scams

Bogdan BOTEZATU – Director of Threat Research @ Bitdefender

Bitdefender

About

- 20 years of experience in cyber-security in several roles
- 16 years under the Draco sign at Bitdefender as director of threat research and reporting
- Best known for the ransomware decryption program
- Coordinates the vulnerability research program and CVE numbering allocation with MITRE.

Bitdefender

Top innovators on the cyber-security scene

- 544 patents for innovation in technology, out of which about 60 are related to AI
- 1800+ employees around the world, out of which 800 working in research and engineering
- Offices in 15 countries, global online presence
- Security Operations Center in San Antonio, Texas & Bucharest, Romania
- Offensive Security and Penetration Testing center in Singapore (Horangi)
- Bitdefender is one of the largest licensors of cyber-security technologies for endpoint and CPMs

Bitdefender

Assisting & Supporting Cybercrime Investigations

2017

Bitdefender advised the Europol's European Cybercrime Centre (EC3), and Europol provided Dutch authorities with an investigation lead into Hansa in 2016.
Read more.

2018

Universal GandCrab decryption tool released for free on No More Ransom (NMR).
Read more.

2019

Europol was assisted by Bitdefender, by advising Europol's European Cybercrime Centre (EC3) on the Silkkitie (known as the Valhalla Marketplace) takedown.
Read more.

The GandCrab decryption tool counters versions 1 and 4 and versions 5 to 5.2
Read more.

2020

Finnish Customs take down Sipulimarket on the dark web with Europol and Bitdefender support.
Read more.

2021

Bitdefender supported the Sodinokibi/REvil ransomware investigation by providing key technical insights throughout the entire investigation, along with decryption tools for both of these highly prolific ransomware families to help victims recover their files.
Read more.

2023

Bitdefender provided additional support that helped with the seizure of PIILOPUOTI.
Read more.

Bitdefender DRACO Team assisted FBI to dismantle IOT proxy for hire used for illegal activities.
Read more.

Bitdefender issued a decryption tool one year earlier, which led to arrests in the LockerGoga Ransomware case.
Read more.

2024

Finnish Customs take down Sipulitie – a dark market responsible for almost $2.2 million on the dark web with Europol and Bitdefender support.
Read more.

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

TULLI
TULL·CUSTOMS

EUROPOL

“Sorry to disturb, I’m looking for a boyfriend for my sister” – here’s how the “fake love” scam works.

Bitdefender

What are deepfakes

Deepfakes used in scams

Spot the fake

New security portfolio

1

Some terminology

Bitdefender

Fraud · Sting · Scam · Con

A scam is a scheme through which a person tries to obtain money, information, or other benefits from a victim by using fraudulent or deceptive methods.

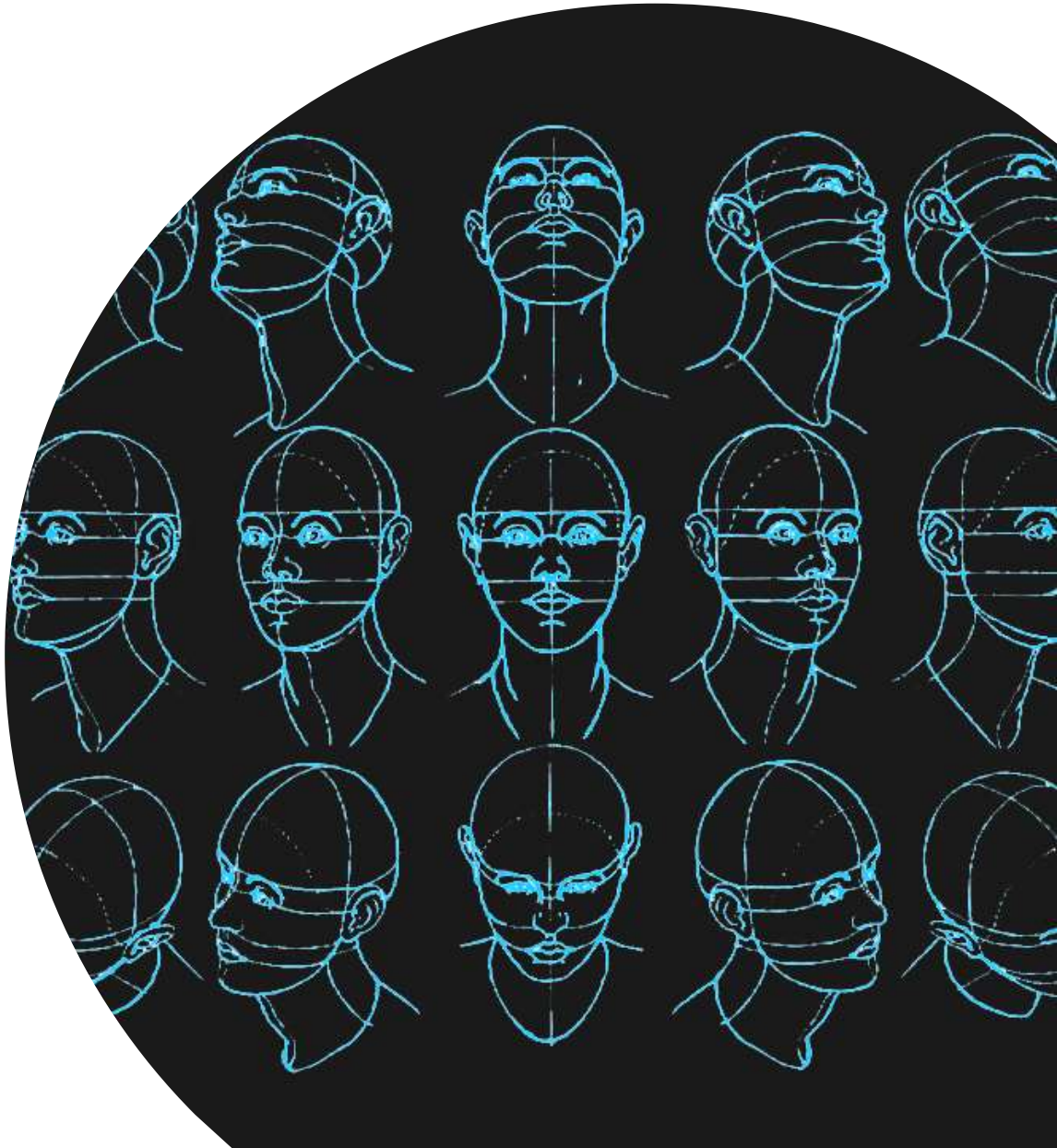
Scammers can employ various strategies, ranging from false promises of large winnings, products or services that don't exist, to phishing attempts to obtain personal and financial data. The ultimate goal is to deceive the victim and exploit them, either financially or through other means.

Bitdefender

Deepfake

A deepfake is a type of digitally manipulated media content, usually video or audio, that uses artificial intelligence (AI) and deep learning techniques to create fake images or sounds that appear real.

In a deepfake video, a person’s face can be replaced with someone else’s, and in audio deepfakes, a person’s voice can be falsified to say things they never actually said.



Bitdefender

Artificial Intelligence

Artificial Intelligence (AI) is a field of computer science that focuses on creating systems capable of performing tasks that normally require human skill and intelligence.

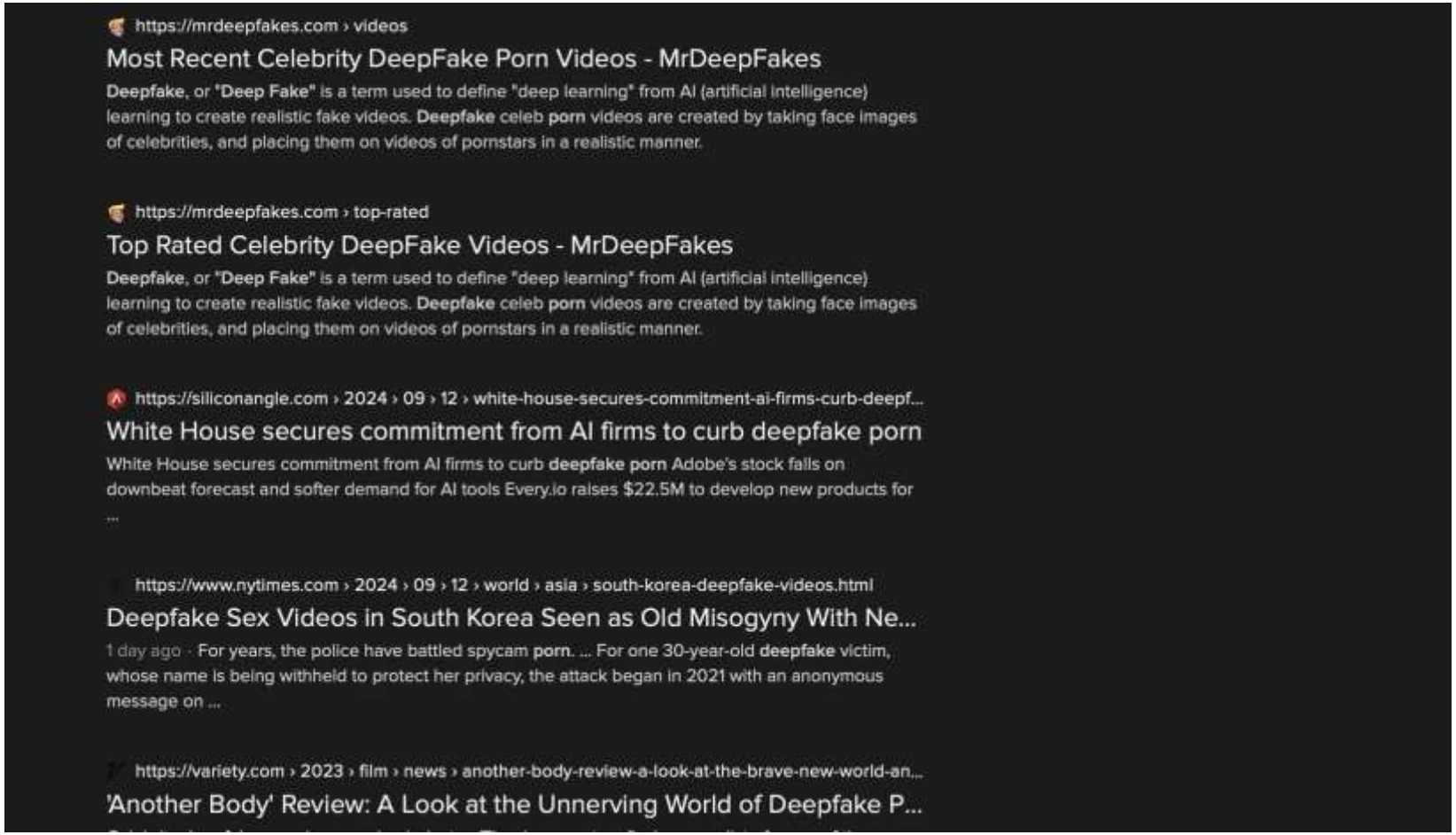
These systems are designed to simulate cognitive processes such as learning, reasoning, visual and language recognition, decision-making, and problem-solving.

Bitdefender

Deepfakes as a form of art

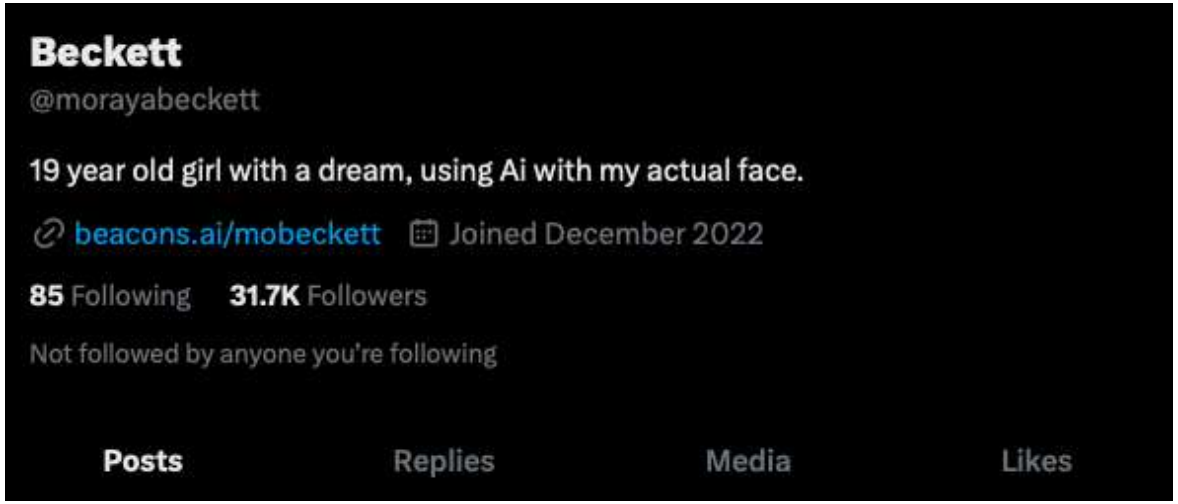
Bitdefender

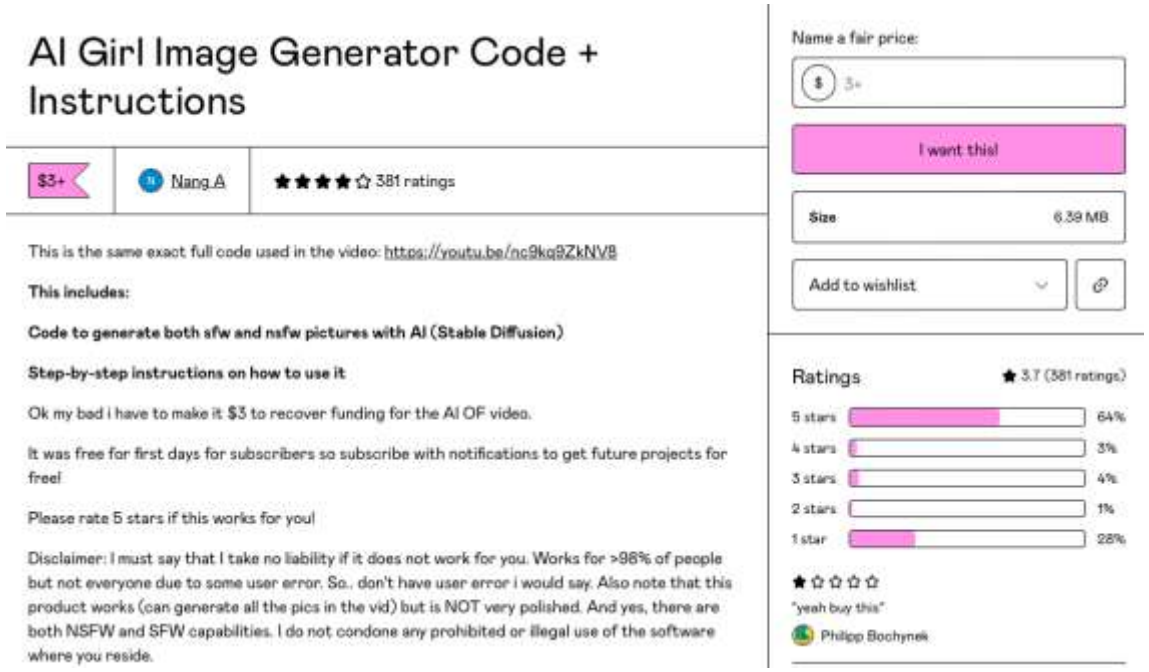
RULE 34



Bitdefender

RULE 34





Bitdefender

NCIIA – Non-Consensual Intimate Image Abuse

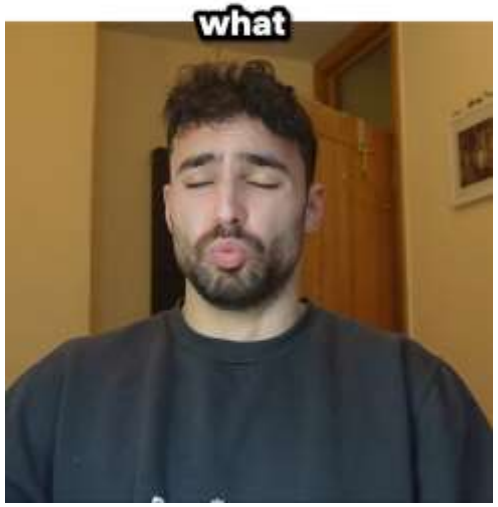
Millions of People Are Using Abusive AI 'Nudify' Bots on Telegram

Bots that "remove clothes" from images have run rampant on the messaging app, allowing people to create nonconsensual deepfake images even as lawmakers and tech companies try to crack down.

Bitdefender

GEN AI can be funny

$$\int_{0.2}^{0.6} x^2 dx$$



Bitdefender

…or downright frightening

2

Deepfakes and cons

Bitdefender

Deepfakes in attacks

Deepfakes allow cybercriminals to create convincing audio or video recordings impersonating high-ranking leaders (such as CEOs or CFOs). These deepfakes are often used in Business Email Compromise (BEC) schemes, where scammers convincingly pose as a company leader, requesting employees to authorize large financial transactions.

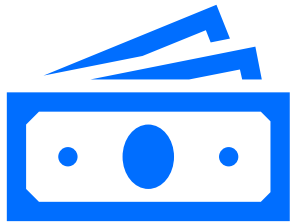
A deepfake voice recording can be used to mimic a CEO’s voice in a phone call with the finance department, asking for an urgent bank transfer.

Deepfake videos of executives can be used in video conferences, enhancing the illusion of legitimacy when requesting sensitive financial actions.

Bitdefender

Attack avenues

Account takeover (ATO)



Paid ads

Short Messages

Bitdefender

Accounts as billboards

Bitdefender

Magnitude

THE GOOD NEWS: IT'S GOING DOWN

- Approx. 10,000 malicious streams identified
- Nearly 6500 channels stolen
- Over 300 malicious domains
- Biggest stolen channel:
  - 12,424,419,842 views (12 billion)
  - over 55,000 videos
  - 28,100,000 subscribers (28 million)

Bitdefender

Landing page

Bitdefender

Deepfakes in attacks against regular people

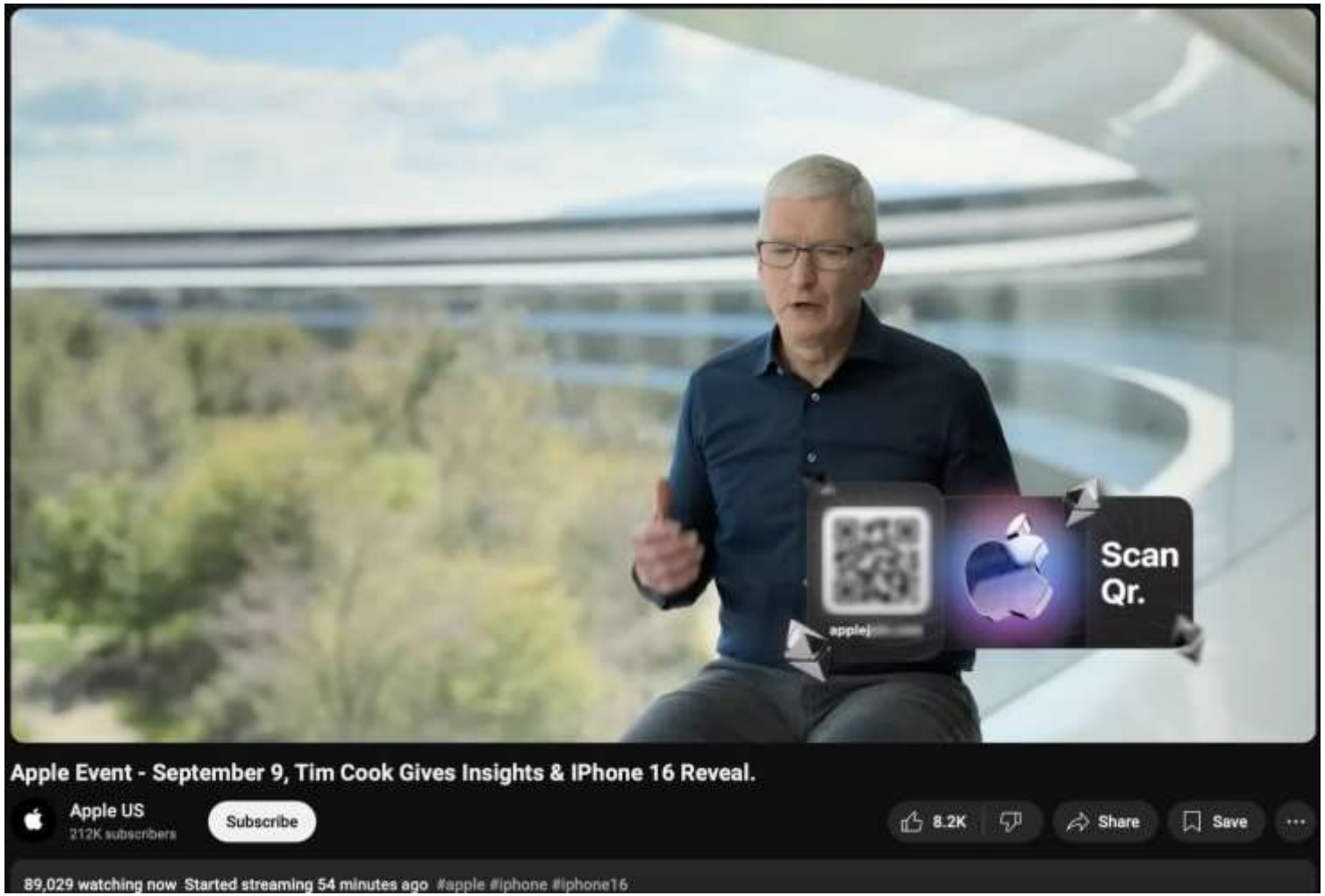
- Good enough for the untrained eye
- Uses a celebrity or public personality easy to recognize by the masses
- Always leverages the idea that they are exposing a secret

Bitdefender

Deepfakes in attacks against regular people

Bitdefender

…and in real time



Bitdefender

Gen AI and scams

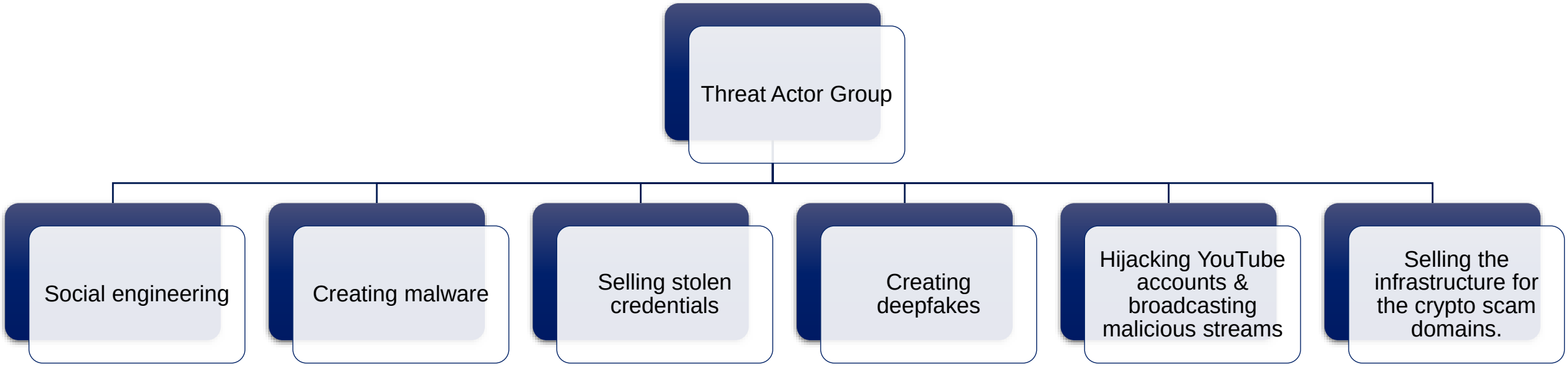
GenAI helps cybercriminals organize complex scams, such as "pig butchering" schemes (a combination of romance and investment scams). Scammers create intricate stories, combining video, audio, and text to set the scene and spark interest.

Often, AI also provides context and localization, enabling scammers from China to target English or Romanian speakers as if they were native speakers.

"Pig butchering" schemes can last for weeks or months, but typically leave the victim penniless and in a dire emotional state.

Bitdefender

Scamming-as-a-Service



Bitdefender

Automated template installation

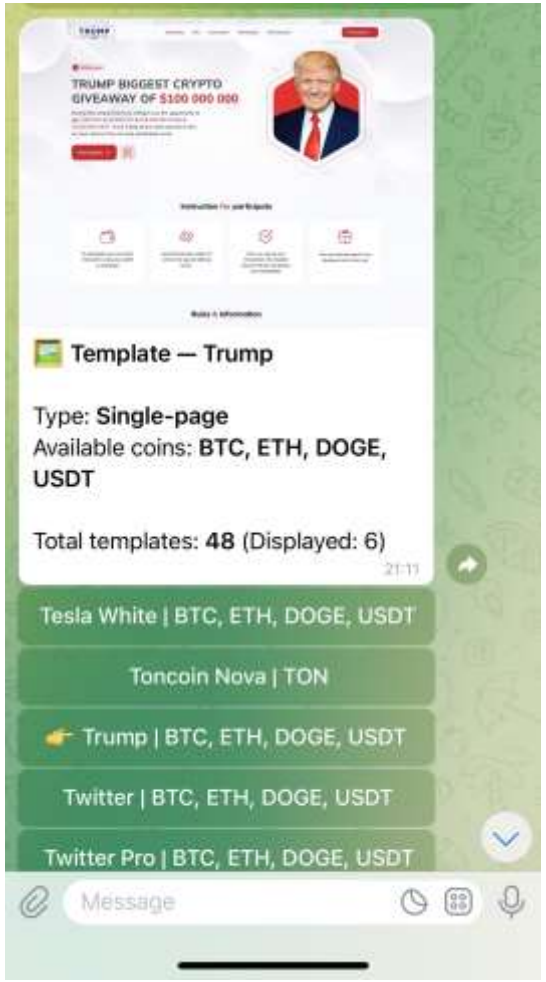
CryptoCore

Powered by CryptoCore
Automatic installation of sites: Telegram @

- Automatic installation of websites in 10 minutes
- Quality templates for different events (25+ templates)
- Easy editing of the site, changing addresses and templates
- Protection against unwanted traffic blocks scanners, the site is harder to block
- Statistics of visits, statistics of copied wallets

Bitdefender

Automated template installation



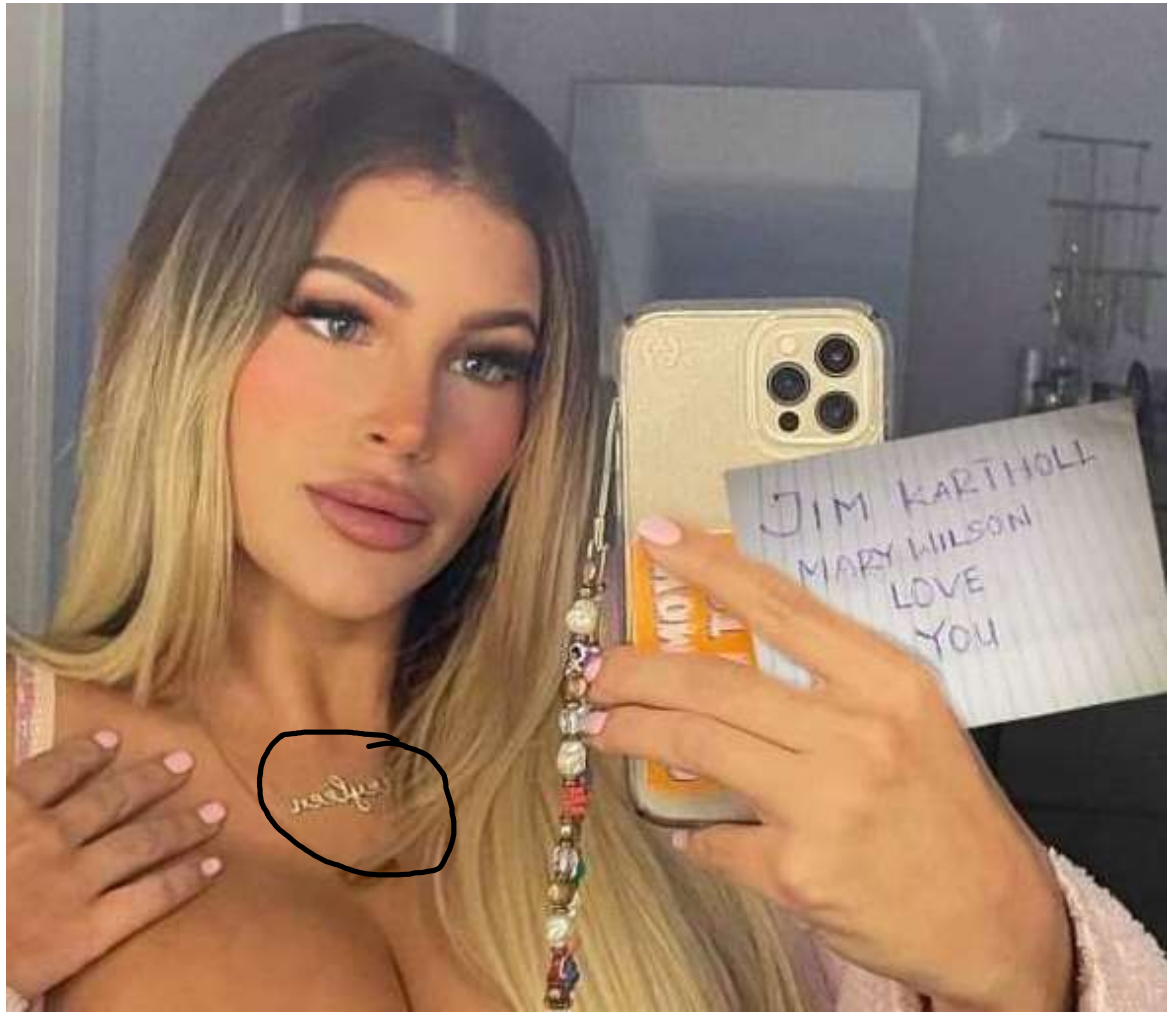
3

SUBTITLE HERE

Spot the fake

Bitdefender

Bitdefender



4

SUBTITLE HERE

New security portfolio

Bitdefender

- NEW **Scam Copilot chatbot** – Specialized AI chatbot ready to help user spot fraudulent intent in suspicious interactions using natural language conversation; across devices.
- NEW **New Scam Wave Alerts** - Proactively informs user about emerging scam activities in their region through the chatbot.
- NEW **Online Scam Protection** – Specialized scam protection in browsing activities to detect new scam patterns and tactics, via Web Protection; across devices.
- **Email Protection** – Protects web mailboxes from Gmail and Outlook providers + local email clients on Windows.
- NEW **Remote Access Scam Protection** - Detects behavior patterns that can enable data loss through remote access apps used by scammers; Windows only .
- IMPROVED **SMS Protection** – AI-infused detection of scam patterns and dangerous links in SMS messages; mobile only.
- **Scam Notification Protection** - Detects scam patterns in notifications from any app on the device; Android only.
- **Chat Protection** - Detects scam patterns in WhatsApp, Facebook Messenger, Telegram and Discord chats; Android only.
- **Calendar Invites Protection** - Detects scam patterns in calendar events; iOS only.
- **Educational layer** – Embedded throughout touch-points
  - Chatbot will provide advice relevant for the user's submitted interaction
  - New detections have an embedded educational component
  - Existing mobile detections with corresponding educational layer
- **Increased shareability**
  - New Scam Wave Alerts include quick actions leading to spreading the news and helping others get protected
  - Existing mobile flows to help others get protected
  - Onboarding promoting installation on all user's devices

Trusted.
Always.