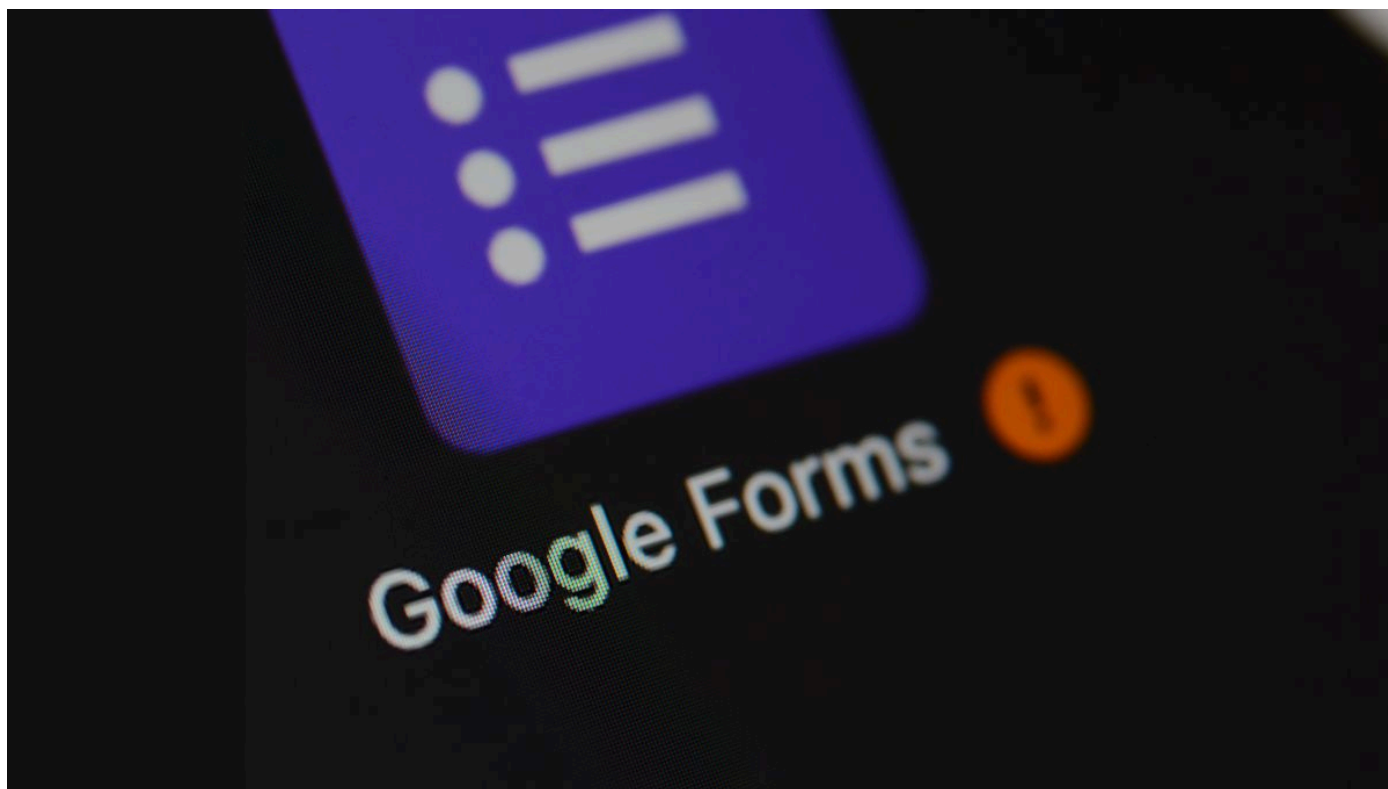


That “job brief” on Google Forms could infect your device

malwarebytes.com/blog/threat-intel/2026/03/that-job-brief-on-google-forms-could-infect-your-device

Gabriele Orini

March 20, 2026



We’ve identified a campaign using business-related lures, such as job interviews, project briefs, and financial document, to distribute malware, including the PureHVNC Remote Access Trojan (RAT).

It’s not the malware that’s new, but how the attack starts.

Instead of the usual phishing email or fake download page, attackers are using Google Forms to kick off the infection chain. The attack typically begins when a victim downloads a business-themed ZIP file linked from a Google Form. Inside is a malicious file that sets off a multi-stage infection process, eventually installing malware on the system.

What is PureHVNC?

PureHVNC is a **modular .NET RAT** from the “Pure” malware family. In simple terms, it gives attackers remote control over an infected device and lets them steal sensitive information.

Once installed, it can:

- Take control of the system and run commands remotely.

- Collect information about the device, including operating system, hardware, security software, and info about the user and connected devices.
- Steal data from browsers, extensions and crypto wallets.
- Extract data from apps like Telegram and Foxmail.
- Install additional plugins.
- Achieve persistence in several ways (for example, via scheduled tasks).

Different lures, same goal: compromise your device

In our research, we found multiple Google Forms hosting links to malicious ZIP files that start the infection chain. These forms are convincing, impersonating real company names, logos and links. LinkedIn is one of the platforms used to send links to these malicious forms.



Project Opportunity: Digital Marketing Specialist – Hisense RGB-Mini LED Evo

Thank you for your interest in joining our global launch campaign. To proceed with the evaluation process, please follow these steps:

1. Review Project Details: Access the full campaign scope, KPIs, timeline, and compensation structure here: [\[LINK TO PROJECT DOCUMENT\]](#)

If your experience aligns with this campaign, we look forward to reviewing your submission.

(For optimal readability, we recommend viewing the document on a desktop or laptop)

2. Submit Your Information: Complete this form so we can assess your fit for this performance-driven role.

Confidentiality Note: All submitted information will be treated as strictly confidential and used solely for evaluation purposes.

We look forward to reviewing your submission!

- Fake Google Forms that distribute malicious ZIPs.

Advertising Partnership Application - Corover AI

Welcome to the Corover AI Partnership Program. We are looking for high-performing advertising experts and agencies to collaborate with us in scaling our market presence. Please fill out the details below, and our team will get back to you within 2-3 business days.

[Accedi a Google](#) per salvare i risultati raggiunti. [Scopri di più](#)

* Indica una domanda obbligatoria

Welcome! We appreciate your interest in joining Corover AI . Please take a moment to complete this form so we can learn more about you. *

☐ Sure

Below is detailed information about our project: *

👉 [Details about Corover AI project](#)

Please review it carefully. If you are interested, kindly complete the form below. We will get in touch with you shortly.*

La tua risposta

- The attackers impersonate real companies

The Ocean Cleanup - 30 Cities Program

- The 2026 Phase

We cordially invite you to participate in this project. However, we would appreciate it if you could answer the following questions, which will help us gain a better mutual understanding and ensure a more effective collaboration in the future. We recommend that you review the project documentation and our proposed salary before responding to the questions below:

Download here:

Document: [[Project Details and Salary Policy Information](#)]

Website: theoceancleanup.com

Should you have any inquiries, please do not hesitate to contact us at hr@theoceancleanup.com, and we will get back to you as soon as possible.

Upon receiving your responses, our support team will contact you to schedule an online meeting to discuss the next steps of our collaboration. We are looking forward to working with you.

[Accedi a Google](#) per salvare i risultati raggiunti. [Scopri di più](#)

* Indica una domanda obbligatoria



- Well-known brands are impersonated to lend credibility

The forms typically ask for professional information (experience, background, etc.), making them feel like part of a real recruitment or business process.

Full Name *

La tua risposta

Location *

La tua risposta

LinkedIn Profile *

La tua risposta

After reviewing the Financial and Salary & Benefits Report, please indicate: *

Do you agree with the proposed salary & Benefits package? (Yes/No)

If No, please write your expected salary.

La tua risposta

- Information requested from the user to make the form appear legitimate.

1. Your Full Name *

La tua risposta

2. Work Email Address *

La tua risposta

3. LinkedIn Profile/ Personal Website/ Portfolio *

La tua risposta

4. Country of Residence *

La tua risposta

5. How many years of experience do you have in your field? *

- ☐ Less than 1 year
- ☐ 1–2 years
- ☐ 3–5 years

- [More information.](#)

The forms link to ZIP files hosted on:

- File-sharing services such as Dropbox, filedn.com, and fshare.vn
- URL shorteners such as tr.ee and goo.su
- Google redirect links that obscure the final destination

The ZIP archives use various names and are tied to different business-related themes (marketing, interviews, projects, job offers, budgets, partnerships, benefits) to avoid suspicion, for example:

- {CompanyName}_GlobalLogistics_Ad_Strategy.zip
- Project_Information_Summary_2026.zip
- {CompanyName} Project 2026 Interview Materials.zip
- {CompanyName}_Company_and_Job_Overview.pdf.rar
- Collaboration Project with {CompanyName} Company 2026.zip

The lures use the names of well-known companies, particularly in the financial, logistic, technology, sustainability and energy sectors. Impersonating legitimate organizations add credibility to their campaign.

What happens after you download the file

The ZIP archives usually contain legitimate files (such as PDFs of job descriptions) and an executable file along with a DLL, typically named `msimg32.dll`. The DLL is executed via DLL hijacking (tricking a legitimate program into loading malicious code), although the technique has undergone multiple modifications and upgrades over time.

JOB DESCRIPTION – ACCOUNTING FINANCE SPECIALIST



Project: MSI Claw 8 AI Plus – International Marketing & Sales Campaign
Work Type: Remote | Part-time | Freelancer
Contract Duration: 2 months (extension based on performance)

1. Role Overview

We are looking for an **Accounting / Finance Specialist** to support the financial operations of the **MSI Claw 8 AI Plus international project**. This role focuses on **budget tracking, expense management, invoicing, and financial reporting** related to marketing and sales activities across multiple international markets. The position is ideal for candidates with experience in **project-based accounting**, international teams, and remote working environments.

2. Key Responsibilities

2.1 Budget & Expense Management

- Track project budgets across marketing, sales, and operational activities.
- Monitor expenses to ensure spending aligns with approved budgets.
- Identify budget variances and flag potential risks early.

2.2 Financial Reporting

- Prepare **weekly and monthly financial reports** related to project spend and performance.
- Maintain accurate records of invoices, payments, and reimbursements.
- Support financial transparency for project stakeholders.

2.3 Invoicing & Payment Coordination

- Manage invoices from freelancers, vendors, and partners.
- Ensure timely payment processing and documentation.
- Coordinate with internal stakeholders regarding payment schedules.

2.4 Accounting Records & Compliance

- Maintain organized accounting records for the project.
- Support basic compliance with internal financial policies and procedures.
- Assist with audit preparation or financial reviews if required.

2.5 Cross-team Collaboration

- Work closely with Project Management, Strategic Planning, and Sales teams.
- Provide financial insights to support decision-making.
- Communicate clearly regarding financial status and updates.

3. Required Qualifications

Must-Have

- 2+ years of experience in **Accounting, Finance, or Bookkeeping**.
- Experience with **project-based or freelance accounting**.
- Strong proficiency in **Excel or Google Sheets**.
- Ability to manage financial data accurately and confidentially.
- Comfortable working remotely with international teams.
- Good command of **English** (written and reading).

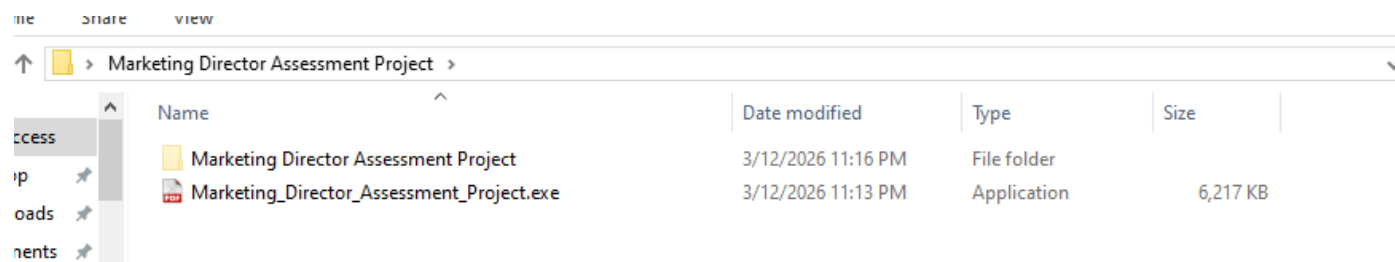
Nice to Have

- Experience supporting marketing or digital projects.
- Familiarity with accounting software (QuickBooks, Xero, or similar).
- Experience handling multi-currency transactions.
- Understanding of basic financial controls and reporting standards.

Legitimate PDFs are present in some ZIP files, like this one masquerading as a real job description.

Analysis of the malicious campaign

We identified multiple variants of this campaign, each using different methods to extract the archive, distinct Python code, and varying folder structures. Across these variants, the campaign typically includes an executable file along with a DLL hidden in a separate folder. In some cases, attackers also include legitimate files related to the lure's theme, enhancing the overall credibility of the attack.



The screenshot shows a Windows File Explorer window with the address bar set to 'Marketing Director Assessment Project'. The left sidebar shows the 'This PC' view. The main pane displays a table of files and folders.

Name	Date modified	Type	Size
Marketing Director Assessment Project	3/12/2026 11:16 PM	File folder	
Marketing_Director_Assessment_Project.exe	3/12/2026 11:13 PM	Application	6,217 KB

Example of files present in one of the archives analyzed.

The malicious code is present in the DLL, and carries out various operations, including:

- Decrypting strings with a simple XOR, in this case with the “4B” key.
- Detecting debugging and sandboxing with `IsDebuggerPresent()` and `time64()`, and displaying the error “This software has expired or debugger detected” if triggered.
- Deleting itself, then dropping and launching a fake PDF.
- Achieving persistence via the registry key `CurrentVersion\Run\Miroupdate`.
- Extracting the “final.zip” archive and running it.

In this case, the PDF was started with the following command:

```
cmd.exe /c start "" "C:\Users\user\Desktop\Marketing Director Assessment
Project\Marketing_Director_Assessment_Project.pdf"
```



Paid Media Campaign – Candidate Assessment

Overview of strategy and execution for success



Agenda Items

- Instructions
- Strategy & Targeting
- Budget
- KPIs
- Creative
- Optimization

The PDF opened during the infection chain.

The archive `final.zip` is unzipped using different commands across the analyzed campaigns into a random folder under `ProgramData`. In this example, the `tar` command is used:

```
cmd.exe /c tar -xf "C:\ProgramData\{random folder}\{random folder \final.zip" -C "C:\ProgramData\{random folder \{random folder} " >nul 2>&1
```

The zip contains several files associated with Python and the next stage.

- `SELECT * FROM Win32_PnPEntity WHERE (PNPClass = 'Image' OR PNPClass = 'Camera')`
- `SELECT Caption FROM Win32_OperatingSystem`

For persistence, it creates a scheduled task using a base64-PowerShell command, with the flag `"-RunLevel Highest"` if the user has admin rights.

```
startInfo = new ProcessStartInfo
{
    FileName = "powershell.exe",
    Arguments = "-NoProfile -ExecutionPolicy Bypass -Enc " + Convert.ToBase64String(Encoding.Unicode.GetBytes(s)),
    UseShellExecute = false,
    CreateNoWindow = true,
    WindowStyle = ProcessWindowStyle.Hidden
};
goto IL_121;
IL_13B:
s = string.Concat(new string[]
{
    "Register-ScheduledTask -TaskName '",
    text,
    "' -Action (New-ScheduledTaskAction -Execute '",
    text2,
    "' -Trigger (New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-TimeSpan -Minutes 5)) -User $env:UserName -Settings (New-
    ScheduledTaskSettingsSet -ExecutionTimeLimit (New-TimeSpan -Seconds 0) -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries) -Force"
});
goto IL_160;
IL_1BC:
if (!Class4.smethod_5())
{
    goto IL_13B;
}
goto IL_160;
IL_1CE:
s = string.Concat(new string[]
{
    "Register-ScheduledTask -TaskName '",
    text,
    "' -Action (New-ScheduledTaskAction -Execute '",
    text2,
    "' -Trigger (New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-TimeSpan -Minutes 5)) -User $env:UserName -RunLevel Highest -
    Settings (New-ScheduledTaskSettingsSet -ExecutionTimeLimit (New-TimeSpan -Seconds 0) -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries) -Force"
});
goto IL_1BC;
IL_202:
goto IL_60;
}
```

PowerShell command for the Scheduled Task

PureHVNC performs enumeration to exfiltrate information related to various browsers, extensions, and cryptocurrency wallets.

```

{
    CS$<>8__locals1.dictionary_0 = new Dictionary<string, string>
    {
        {
            "ibnejdfjmmkpcnlpebklmnkoeiohofec",
            "TronLink"
        },
        {
            "nkbihfbeogaeaoehlefnkodbefgpgknn",
            "MetaMask"
        },
        {
            "fhbohimaebolbohpbldcngcnapndodjp",
            "Binance Chain Wallet"
        },
        {
            "ffnbelfdoeiohenkjibnmadjiehjhajb",
            "Yoroi"
        },
        {
            "cjelfplplebdjjenllpjcbmljkfcffne",
            "Jaxx Liberty"
        },
        {
            "fihkakfobkmkjojpchpfgcmhfjnmnfpi",
            "BitApp Wallet"
        },
        {
            "kncchdigobghenbbaddojjnaogfppfj",
            "iWallet"
        },
        {
            "aiifbnfbobpmeekipheeiimdpnlpgpp",
            "Terra Station"
        },
        {
            "ijmpgkjfkbfhoebgogflfebnejmfbml",
            "BitClip"
        },
        {
            "blnieiiffboillknjnpogjhgknoapac",
            "EQUAL Wallet"
        }
    }
}

```

```

};
Dictionary<string, string> dictionary = new Dictionary<string, string>();
dictionary.Add("Chromium\\User Data\\", "Chromium");
dictionary.Add("Google\\Chrome\\User Data\\", "Chrome");
dictionary.Add("Google(x86)\\Chrome\\User Data\\", "Chrome");
dictionary.Add("BraveSoftware\\Brave-Browser\\User Data\\", "Brave");
dictionary.Add("Microsoft\\Edge\\User Data\\", "Edge");
dictionary.Add("Tencent\\QQBrowser\\User Data\\", "QQBrowser");
dictionary.Add("MapleStudio\\ChromePlus\\User Data\\", "ChromePlus");
dictionary.Add("Iridium\\User Data\\", "Iridium");
dictionary.Add("7Star\\7Star\\User Data\\", "7Star");
dictionary.Add("CentBrowser\\User Data\\", "CentBrowser");
dictionary.Add("Chedot\\User Data\\", "Chedot");
dictionary.Add("Vivaldi\\User Data\\", "Vivaldi");
dictionary.Add("Kometa\\User Data\\", "Kometa");
dictionary.Add("Elements Browser\\User Data\\", "Elements");
dictionary.Add("Epic Privacy Browser\\User Data\\", "Epic Privacy");
dictionary.Add("uCozMedia\\Uran\\User Data\\", "Uran");
dictionary.Add("Fenrir Inc\\Sleipnir5\\setting\\modules\\ChromiumViewer\\", "Sleipnir5");
dictionary.Add("CatalinaGroup\\Citrio\\User Data\\", "Citrio");
dictionary.Add("Coowon\\Coowon\\User Data\\", "Coowon");
dictionary.Add("liebao\\User Data\\", "liebao");
dictionary.Add("QIP Surf\\User Data\\", "QIP Surf");
dictionary.Add("Orbitum\\User Data\\", "Orbitum");
dictionary.Add("Comodo\\Dragon\\User Data\\", "Dragon");
dictionary.Add("Amigo\\User\\User Data\\", "Amigo");
dictionary.Add("Torch\\User Data\\", "Torch");
dictionary.Add("Comodo\\User Data\\", "Comodo");
dictionary.Add("360Browser\\Browser\\User Data\\", "360Browser");
dictionary.Add("Maxthon3\\User Data\\", "Maxthon3");
dictionary.Add("K-Melon\\User Data\\", "K-Melon");
dictionary.Add("Sputnik\\Sputnik\\User Data\\", "Sputnik");
dictionary.Add("Nichrome\\User Data\\", "Nichrome");
dictionary.Add("CocCoc\\Browser\\User Data\\", "CocCoc");
dictionary.Add("Uran\\User Data\\", "Uran");
dictionary.Add("Chromodo\\User Data\\", "Chromodo");
dictionary.Add("Mail.Ru\\Atom\\User Data\\", "Atom");
CS$<8_locals1.object_0 = new object();
Parallel.ForEach<KeyValuePair<string, string>>(dictionary, new Action<KeyValuePair<string, string>>(CS$<8_locals1.method_0));
}

```

Methods related to wallet and browser data exfiltration.

The malware configuration is encoded with base64 and compressed with GZIP.

In this case, the configuration includes:

- **C2:** 207.148.66.14
- **C2 ports:** 56001, 56002, 56003
- **Campaign ID:** Default
- **Sleeping Flag:** 0
- **Persistence Path:** APPDATA
- **Mutex Name:** Rluukgz

How to stay safe

Using Google Forms is a highly effective method for distributing malware. Attackers are relying on trust in familiar tools like Google Forms, Dropbox, and LinkedIn, and impersonating legitimate companies to get past your guard.

If you deal with job offers, partnerships, or project work online, this is worth paying attention to:

- Always check the origin of Google Forms, don't enter sensitive information, and don't download files unless you fully trust the source.

- Verify requests through official company channels before engaging.
- Be wary of links hidden behind URL shorteners or redirects.

Indicators of Compromise (IOCs)

IP

207.148.66.14

URL

[https://goo\[.\]su/CmLknt7](https://goo[.]su/CmLknt7)

[https://www.fshare\[.\]vn/file/F57BN4BZPC8W](https://www.fshare[.]vn/file/F57BN4BZPC8W)

[https://tr\[.\]ee/R9y0SK](https://tr[.]ee/R9y0SK)

[https://dl.dropbox\[.\]com/scl/fi/52sgtk50j285hmde2ycry/Overview-of-the-MSI-Accounting-Project.rar?rlkey=9qmunvcp8oleeycld08gqwup9](https://dl.dropbox[.]com/scl/fi/52sgtk50j285hmde2ycry/Overview-of-the-MSI-Accounting-Project.rar?rlkey=9qmunvcp8oleeycld08gqwup9)

HASH

ca6bd16a6185c3823603b1ce751915eaa60fb9dcef91f764bef6410d729d60b3
d6b7ab6e5e46cab2d58eae6b15d06af476e011a0ce8fcb03ba12c0f32b0e6386
e7b9f608a90bf0c1e477a28f41cb6bd2484b997990018b72a87268bf46708320
e221bb31e3539381d4753633443c1595bd28821ab6c4a89ad00ea03b2e98aa00
7f9225a752da4df4ee4066d7937fe169ca9f28ecddf76aa5151fb72a57d54b
e0ced0ea7b097d000cb23c0234dc41e864d1008052c4ddaeaea85f81b712d07c
b18e0d1b1e59f6e61f0dcab62fecebd8bcf4eb6481ff187083ea5fe5e0183f66
85c07d2935d6626fb96915da177a71d41f3d3a35f7c4b55e5737f64541618d37
b78514cfd0ba49d3181033d78cb7b7bc54b958f242a4ebcd0a5b39269bdc8357
fe398eb8dcf40673ba27b21290b4179d63d51749bc20a605ca01c68ee0eaebbc
1d533963b9148b2671f71d3bee44d8332e429aa9c99eb20063ab9af90901bd4d
c149158f18321badd71d63409d08c8f4d953d9cd4a832a6baca0f22a2d6a3877
83ce196489a2b2d18a8b17cd36818f7538128ed08ca230a92d6ee688cf143a6c
ea4fb511279c1e1fac1829ec2acff7fe194ce887917b9158c3a4ea213abd513a
59362a21e8266e91f535a2c94f3501c33f97dce0be52c64237eb91150eee33e3

a92f553c2d430e2f4114cfadc8e3a468e78bdadc7d8fc5112841c0fdb2009b2a
4957b08665d8bb6a2d7f81bf1d96d252c4d8c1963de228567d6d4c73858803a4
481360f518d076fc0acb671dc10e954e2c3ae7286278dfe0518da39770484e62
8d6bc4e1d0c469022947575cbdb2c5dd22d69f092e696f0693a84bc7df5ae5e0
258adaed24ac6a25000c9c1240bf6834482ef62c22b413614856b8973e11a79f

Pro tip: This is only a partial list of malicious URLs. Download the [Malwarebytes Browser Guard plugin](#) for full protection and to block the remaining malicious domains.

We don't just report on threats—we remove them

Cybersecurity risks should never spread beyond a headline. Keep threats off your devices by [downloading Malwarebytes today](#).