

When Malware Wears a Brand: Zoom Lure → Fake Microsoft Marketplace → Remote Access via Zoho

 cyberarmor.tech/blog/zoom-meeting-phish-fake-microsoft-marketplace-zoho-remote-access-brand-impersonation-attack

Nguyen Nguyen

April 22, 2026

 When Malware Wears a Brand: Zoom Lure → Fake Microsoft Marketplace → Remote Access via Zoho

Overview

We recently detected an active campaign using a Zoom-themed lure to deliver malware. A deeper analysis shows a shift in attacker tradecraft: combining trusted brands, legitimate tools, and newly created impersonation domains to register as a real business on commercial platforms and execute the attack. This is not a simple drop-and-run campaign, but a structured operation with planning and intent. Figure 1 shows the attack flow.

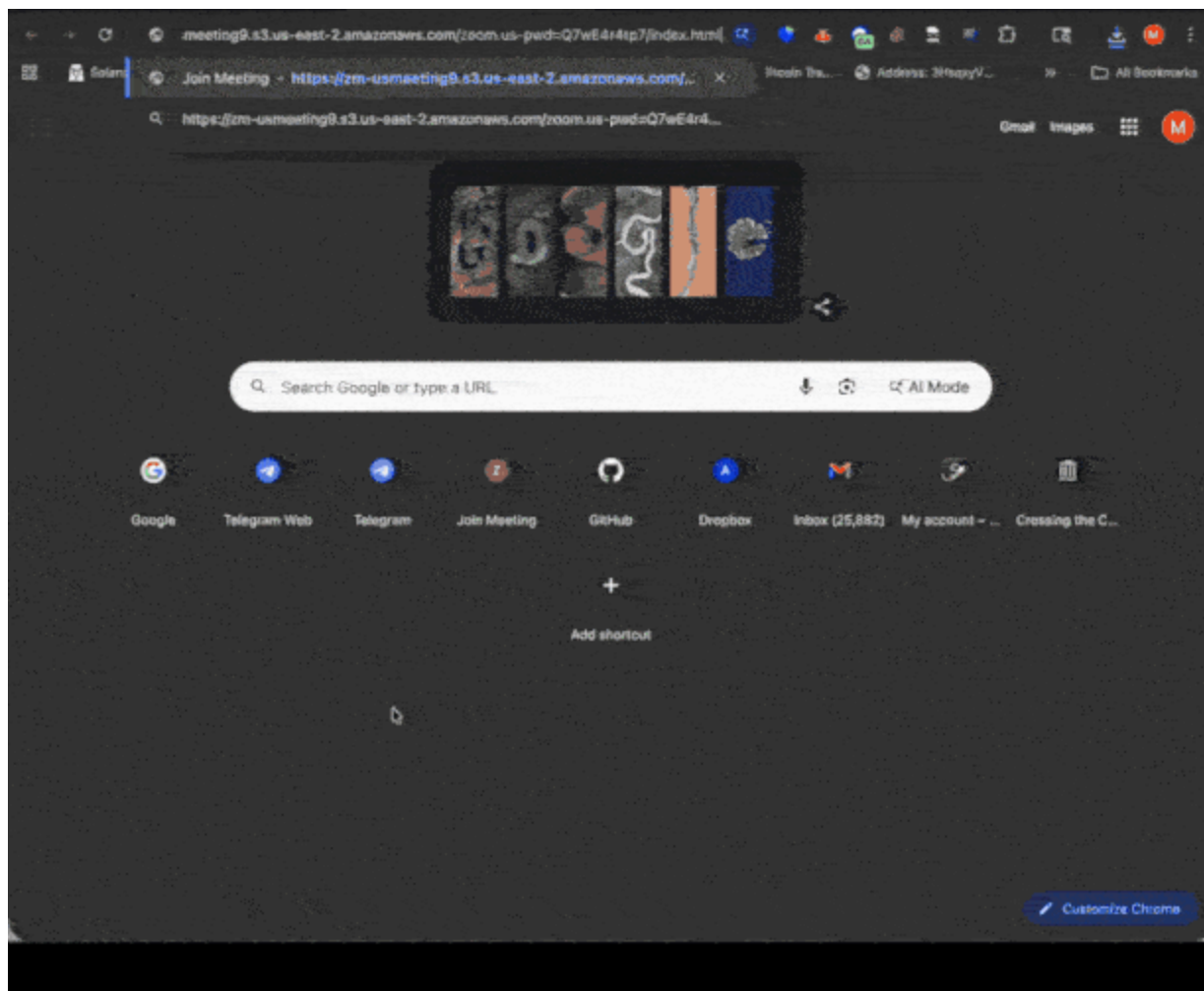


Figure 1: Attack flow

Attack Chain Overview

1. Initial lure - Zoom meeting theme
2. Show the meeting is ongoing (3 participants)
3. Joining the zoom meeting
4. Show Zoom Client is out of date
5. Show Microsoft Store with Zoom Install button
6. Download ZoomWorkplaceSetup.exe
7. Show direction to install the software

Binary overview

The **ZoomWorkplacesSetup.exe** file is a Zoho Assist Unattended Agent. This software enables persistent remote access to Windows, macOS, Linux, and Android devices without requiring a user to be present. As a result, once installed, a cybercriminal can maintain continuous access to the victim's machine. The software have the following properties:

MD5: 4207272b05d5cd9a0736daccbe9b8c65

SHA1: 1f5d4574b956dfcf9c7d4c2d85c42cdb5a042fd6

SHA256: 96d17638013a8d1d2029c5ecc97a0c583039f243e88afb7a6f3adc8b30c0061c

Upon inspection, the agent contains configuration details tied to its owner (the cybercriminal).

- email:info@ceda-rock.com
- unattended_device_register:wSsVR60g8kamWK10nWGtILw+yFRTVQz+E0143lqj6SSqHq/Fp8dvIRHHBFOvHPIYFDU6EjtD8r8tmxIV2zEK2tl5yF4ECCiF9mqRe1U4J3x1prrpIDDKW21dkxOILloOxwxvng==
- webServer:assist.zoho.com
- productId:1
- src:SINGLE_DEPLOYMENT
- proxy_details:{"type":0}
- org_id:921094852

- orgId:b501306e79ddcb5199ef6f502b6f7f2f77e63ab65f4e7d6befa0346d36d22f0d
- gatewayName:gwwa.zohoassist.com
- gatewayPort:443
- gatewayWebServer:wa2.zohoassist.com

Brand Impersonating

As shown in the configuration of the Zoho Assist agent, the owner is associated with organization ID 921094852 and the email address info@ceda-rock[.]com. Based on VirusTotal data, the domain was registered nine days ago and currently hosts an active website. Figure 2 shows the domain creation date from VirusTotal, and Figure 3 shows the current webpage for the domain.

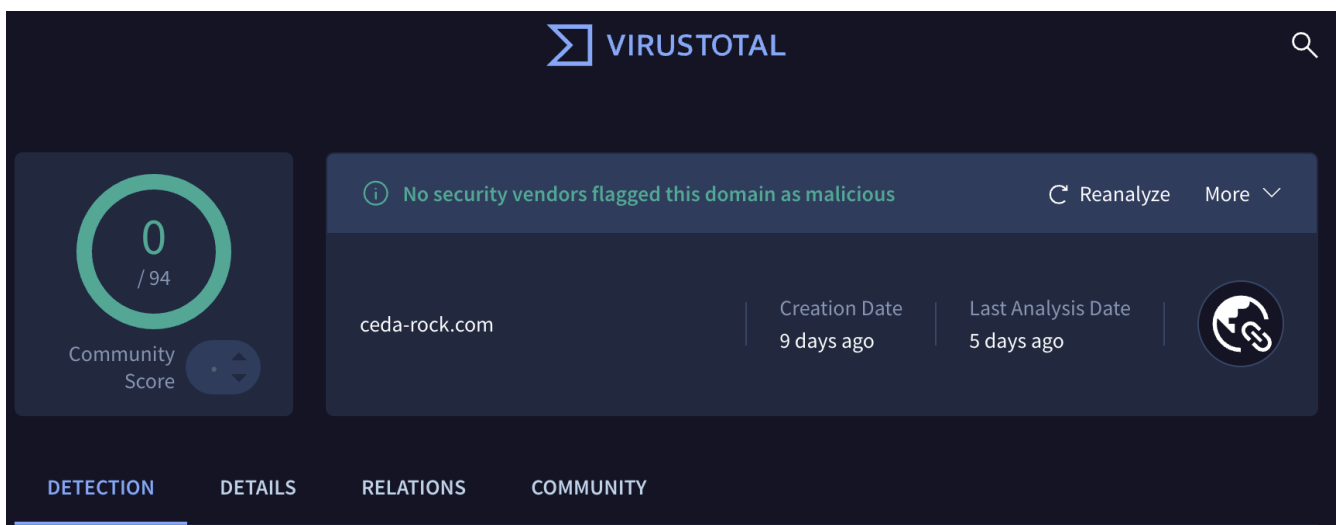
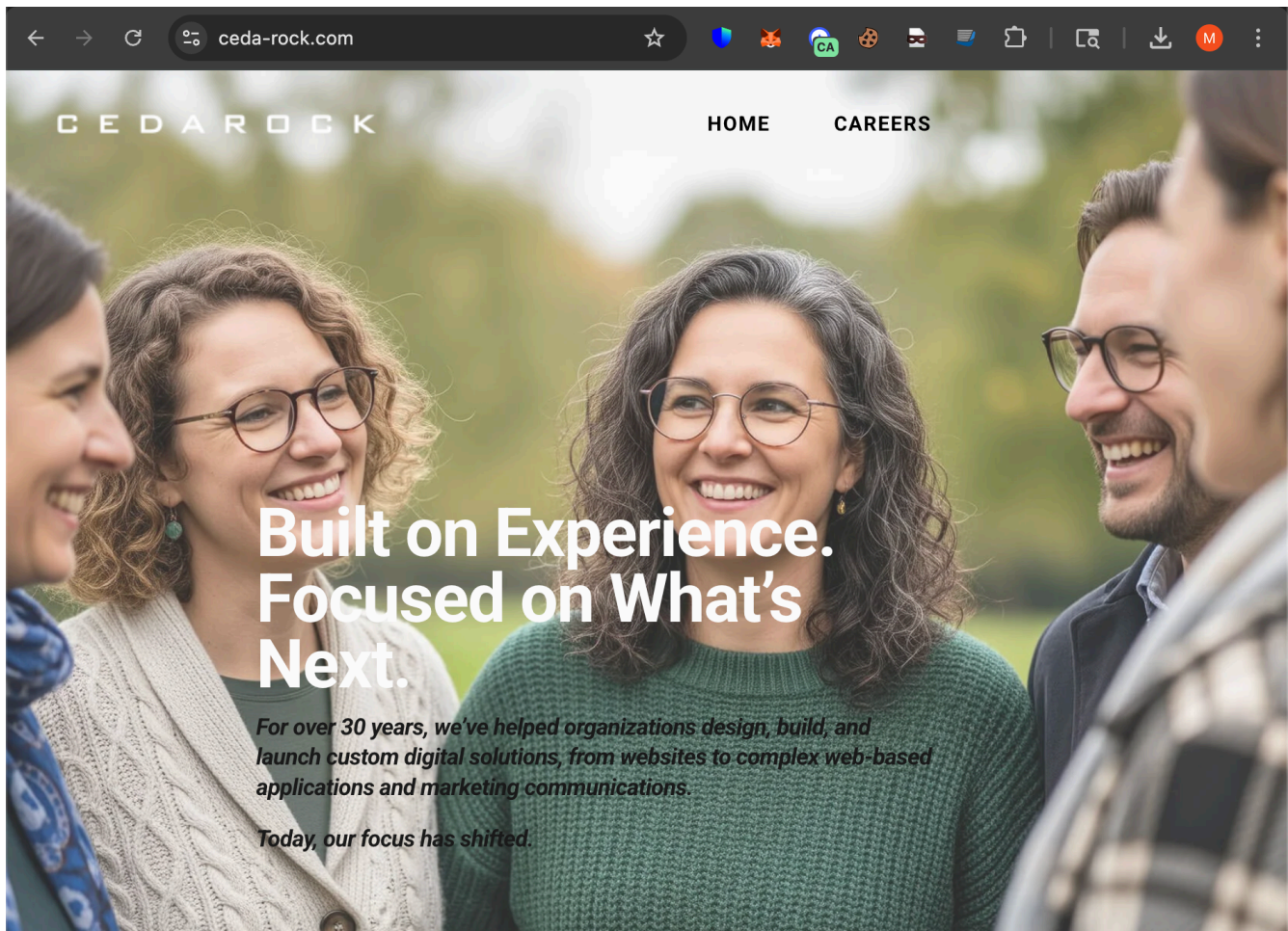


Figure 2: ceda-rock[.] creation date



What We Do

We specialize in:



Upon inspecting the website, the scammer links their “LinkedIn” profile to the legitimate brand, reinforcing credibility and revealing the target of impersonation: cedarrock.com. This provides insight into the operation: to leverage a trusted platform like Zoho Assist, the actor creates and impersonates a real brand, then uses the lookalike domain to register a Zoho account and deploy the agent as a backdoor. This approach helps obscure attribution and reduces the likelihood of being flagged.

Why This Works

1) Abuse of Legitimate Software

Using Zoho Meeting avoids typical malware signatures. Security controls often treat it as benign, allowing:

- Interactive session control
- Screen visibility
- Potential credential harvesting or lateral movement

2) Brand Stacking

The attack layers multiple trusted brands:

- Zoom (entry point)
- Microsoft (delivery trust anchor)
- Zoho (execution mechanism)

Each step reduces suspicion and increases conversion.

3) Domain Impersonation at Scale

The domain **ceda-rock.com** was registered recently and mimics **cedarock.com** (legitimate entity).

This is a classic **typosquatting + brand impersonation** model:

- Minimal visual difference
- Short domain age
- Rapid deployment of a themed website

Defensive Considerations

- block all new domains
- application whitelisting
- Educate users on **meeting-based social engineering**
- Your brand is now part of the attack chain
- Protection requires **external monitoring**, not just internal security
- Early detection reduces both fraud and reputational damage

Conclusion

Over the past few months, there has been an increase in attacks leveraging legitimate commercial tools to gain and maintain access to victim machines. Platforms such as ScreenConnect and ConnectWise are being abused, with cybercriminals creating accounts and deploying them in campaigns themed around entities like the Social Security Administration. Because these tools are legitimate, their use often goes unnoticed.

This campaign reflects a broader evolution:

Attackers are no longer relying solely on malware sophistication—they are **engineering trust**.

By combining:

- Familiar collaboration workflows
- Recognizable platforms
- Newly created impersonation domains

they bypass both technical controls and human skepticism.

The priority is shifting from “**detect malware**” to “**detect deception at scale**.”

IOCs:

zm-usmeeting9[.]s3.us-east-2.amazonaws[.]com/zoom.us-pwd=Q7wE4r4tp7/index.html

ceda-rock[.]com

4207272b05d5cd9a0736daccbe9b8c65

1f5d4574b956dfcf9c7d4c2d85c42cdb5a042fd6

96d17638013a8d1d2029c5ecc97a0c583039f243e88afb7a6f3adc8b30c0061c

Want to detect threats 8+ months earlier?

See how DarkArmor's PreBreach intelligence can protect your organization.

[Book a Demo](#)

 Nguyen Nguyen

About the Author

Nguyen Nguyen

Nguyen (Founder & CEO @ CyberArmor) is a seasoned cybersecurity leader with over 15 years of experience in software engineering, malware research, and cyber threat intelligence.

[LinkedIn Profile](#)