
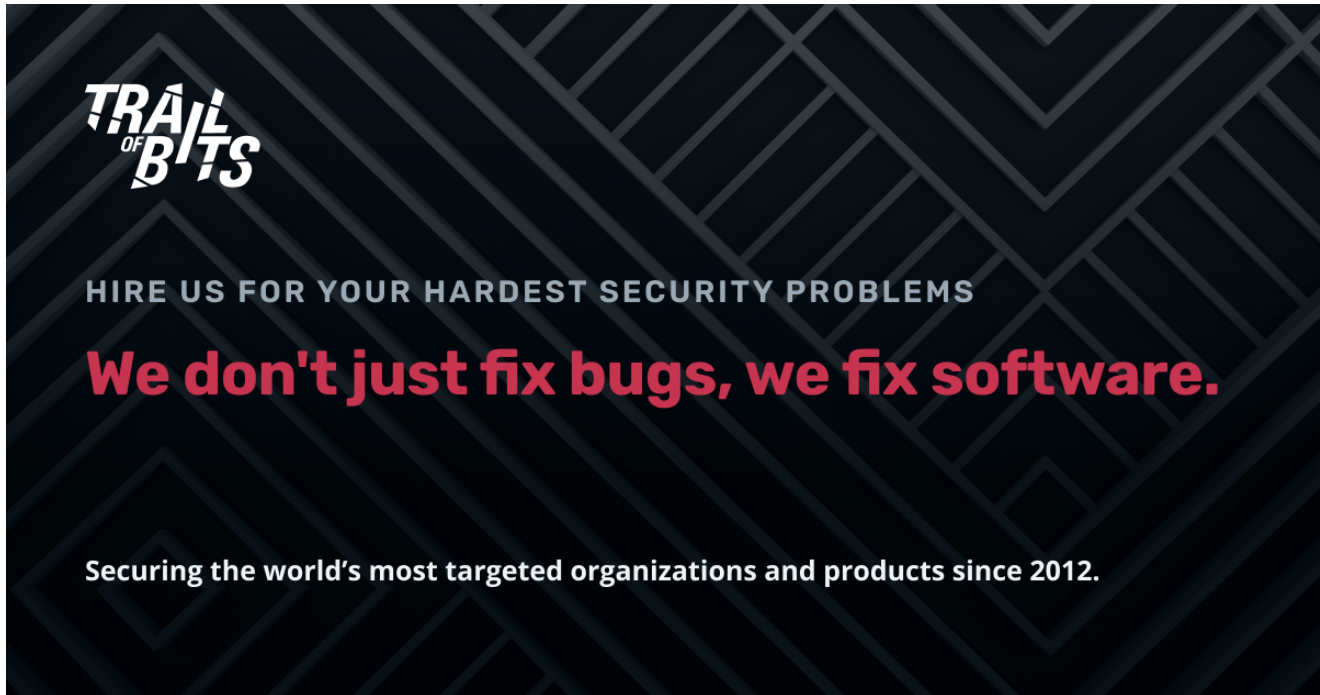


Mitigating ELUSIVE COMET Zoom remote control attacks

 blog.trailofbits.com/2025/04/17/mitigating-elusive-comet-zoom-remote-control-attacks/

April 17, 2025



When our CEO received an invitation to appear on “Bloomberg Crypto,” he immediately recognized the hallmarks of a sophisticated social engineering campaign. What appeared to be a legitimate media opportunity was, in fact, the latest operation by [ELUSIVE COMET](#)—a threat actor responsible for millions in cryptocurrency theft through carefully constructed social engineering attacks.

This post details our encounter with ELUSIVE COMET, explains their attack methodology targeting the Zoom remote control feature, and provides concrete defensive measures organizations can implement to protect themselves.

Our encounter with ELUSIVE COMET

Two separate Twitter accounts approached our CEO with invitations to participate in a “Bloomberg Crypto” series—a scenario that immediately raised red flags. The attackers refused to communicate via email and directed scheduling through Calendly pages that clearly weren’t official Bloomberg properties. These operational anomalies, rather than technical indicators, revealed the attack for what it was.



X DMs between Dan Guido (Trail of Bits CEO) and sockpuppet accounts from ELUSIVE COMET

The ELUSIVE COMET methodology mirrors the techniques behind the recent \$1.5 billion Bybit hack in February, where attackers manipulated legitimate workflows rather than exploiting code vulnerabilities. This reinforces our perspective that the blockchain industry has entered [the era of operational security failures](#), where human-centric attacks now pose greater risks than technical vulnerabilities.

New ELUSIVE COMET IoCs

In addition to the IoCs previously published in [SEAL's advisory on ELUSIVE COMET](#), we have identified new accounts associated with this threat actor's infrastructure:

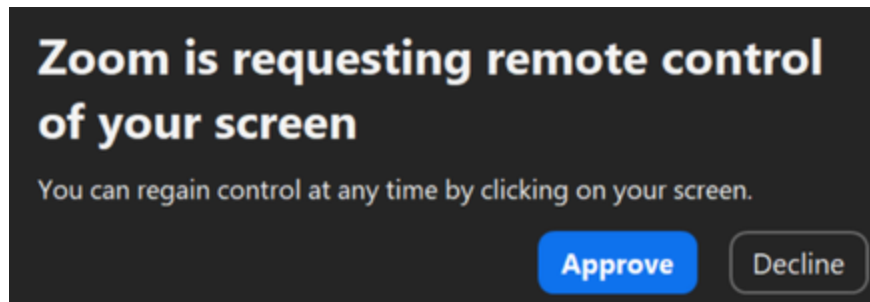
- X: @KOanhHa
- X: @EditorStacy
- Email: bloombergconferences\[@\]gmail.com
- Zoom URL: [https://us06web\[.\]zoom\[.\]us/j/84525670750](https://us06web[.]zoom[.]us/j/84525670750)
- Calendly URL: [calendly\[.\]com/bloombergseries](https://calendly[.]com/bloombergseries)
- Calendly URL: [calendly\[.\]com/cryptobloomberg](https://calendly[.]com/cryptobloomberg)

Organizations should update their monitoring systems and blocklists to include these new indicators.

Understanding Zoom's remote control feature

ELUSIVE COMET's primary attack vector leverages Zoom's remote control feature—a legitimate function that allows meeting participants to control another user's computer with permission. When a participant requests remote control, the dialog simply states

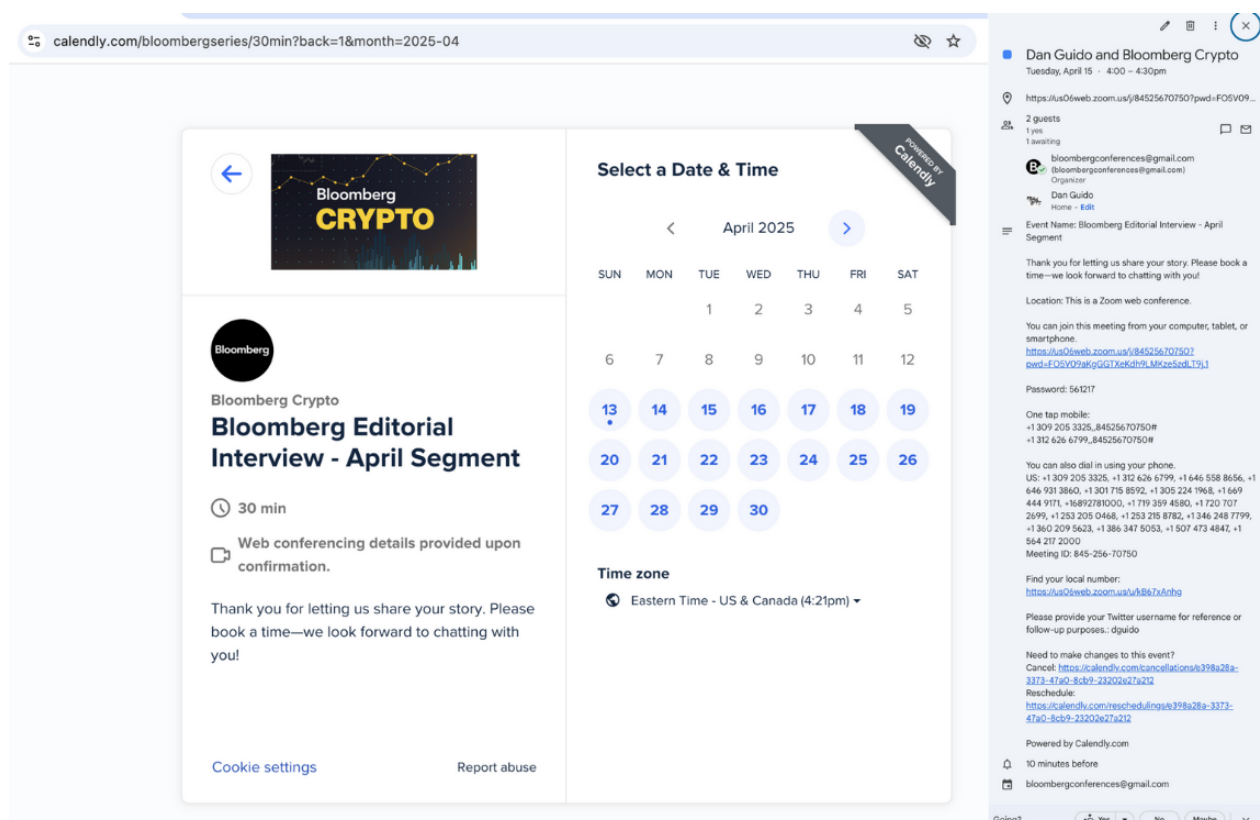
“\$PARTICIPANT is requesting remote control of your screen.”



Example of the Zoom remote control request dialog showing a forged name 'Zoom' as the requester

The attack exploits this feature through a simple yet effective social engineering trick:

1. The attacker schedules a seemingly legitimate business call.
2. During screen sharing, they request remote control access.
3. They change their display name to “Zoom” to make the request appear as a system notification.
4. If granted access, they can install malware, exfiltrate data, or conduct cryptocurrency theft.



Calendly booking page used by the attackers to schedule fake Bloomberg interviews and meeting invite from 'Bloomberg Crypto'

What makes this attack particularly dangerous is the permission dialog's similarity to other harmless Zoom notifications. Users habituated to clicking "Approve" on Zoom prompts may grant complete control of their computer without realizing the implications.

Why this attack succeeds (even against security professionals)

The ELUSIVE COMET campaign succeeds through a sophisticated blend of social proof, time pressure, and interface manipulation that exploits normal business workflows:

- **Legitimate context:** The attack occurs during what appears to be a normal business interaction.
- **Interface ambiguity:** The permission dialog doesn't clearly communicate the security implications.
- **Habit exploitation:** Users accustomed to approving Zoom prompts may act automatically.
- **Attention division:** The victim is focused on a professional conversation, not security analysis.

This approach targets operational security boundaries rather than technical vulnerabilities.

Trail of Bits' defense posture

Our encounter with ELUSIVE COMET reinforces our belief in defense-in-depth strategies that address both technical and operational security domains:

- **Endpoint protection:** [CrowdStrike Falcon Complete](#) with 24/7 managed hunting and response, configured in the "Active" security posture with aggressive cloud and sensor-based ML prevention settings. This configuration enables real-time behavioral detection of suspicious process activities—particularly unauthorized attempts to access system accessibility features—even when the malware is previously unknown or fileless.
- **OS security:** Mandatory company-wide upgrades to the latest major macOS version once its .1 release becomes available. Apple consistently narrows attack surfaces with each major OS release, introducing features that mitigate classes of vulnerabilities rather than just patching individual bugs. This zero-tolerance approach to legacy macOS versions strengthens our security baseline.
- **Authentication hardening:** Mandatory security key authentication for all Google Workspace accounts. Every employee receives a YubiKey during onboarding with zero exceptions granted for weaker authentication methods (TOTP, SMS, etc.). Google SSO serves as our primary authentication provider, extending this hardware-based phishing resistance to all supported services. This implementation creates a hard security boundary that even sophisticated social engineering can't bypass.

- **Password management:** [1Password](#) deployed company-wide with preinstalled browser extensions for all employees. The extension's domain-matching logic prevents credential autofill on mismatched domains (e.g., g00gle.com vs google.com), creating deliberate friction when employees encounter potential phishing sites. This forces a conscious copy-paste action for credentials on suspicious domains—a simple but effective cognitive interrupt that triggers security awareness.
- **Communication platform choices:** Primary use of Google Meet over Zoom due to its browser-based security model. Browser-based communication tools inherit the security model of the browser itself, limiting their access to system resources. Chrome's sandbox prevents web applications from accessing local system resources without explicit permission, creating a more controlled execution environment than installed applications can provide.
- **Restrictive application controls:** When Zoom is required, it's wrapped with additional security controls and routinely removed from systems. Through threat intelligence and our own security research, we identify high-risk applications that are frequently abused in attacks. We apply additional controls to these "tallest blades of grass" to limit their access to system resources and regularly remove them when not actively needed.

Most critically, our security team has identified the Zoom remote control feature as an unnecessary risk and deployed technical controls to prevent it from functioning on our systems. By specifically targeting the accessibility permissions that enable remote control, we close the attack vector that ELUSIVE COMET exploits without disrupting legitimate videoconferencing functionality.

A layered defense approach

To protect your organization from this attack vector, we recommend using [our tools](#) to implement multiple layers of protection:

Script	Purpose	Execution Frequency	Target Scope
<code>create_zoom_pppc_profile.bash</code>	Creates system-wide PPPC profiles that prevent accessibility access	Once per computer	All computers
<code>disable_zoom_accessibility.bash</code>	Actively checks and removes Zoom accessibility permissions	Every 15 minutes	Computers with Zoom installed
<code>uninstall_zoom.bash</code>	Completely removes removal of Zoom from fleet computers	Weekly	Computers with Zoom installed

System-wide protection with PPC profiles

Privacy Preferences Policy Control (PPPC) profiles provide the strongest protection by preventing Zoom from requesting or receiving accessibility permissions at the macOS system level. This directly addresses the vulnerability because Zoom's remote control feature requires accessibility permissions to function—without these permissions, the remote control capability is completely disabled, neutralizing ELUSIVE COMET's primary attack vector.

PPPC profiles offer several security advantages:

- Apply to all users on a system, including new user accounts
- Cannot be removed by regular users once installed
- Enforce organizational security controls regardless of user preferences
- Specifically target only the official Zoom application using code signature verification

The profile works by explicitly denying accessibility permissions to Zoom at the system level, creating a permission boundary that users cannot override through normal means. This approach is particularly effective because it doesn't rely on user vigilance or training—it simply makes the vulnerable functionality technically impossible to enable.

When deployed organization-wide, these profiles ensure consistent protection even when users are under pressure during high-stakes business conversations. By focusing specifically on removing the accessibility permissions that the remote control feature requires, this protection doesn't interfere with legitimate Zoom videoconferencing functionality while still preventing the specific attack vector that ELUSIVE COMET exploits.

Active defense with TCC database monitoring

While PPC profiles provide proactive protection for new permission requests, they don't automatically revoke permissions that users have already granted to Zoom. This is where active TCC database monitoring becomes critical - it functions as a "permission reset" mechanism that continuously cleans up existing accessibility authorizations that could be exploited.

The `disable_zoom_accessibility.bash` script works by directly interfacing with macOS's Transparency, Consent and Control (TCC) framework to methodically:

- Detect existing accessibility permissions granted to Zoom
- Reset those permissions, regardless of when or how they were granted
- Create security telemetry through logging for detection of potential attack attempts

This approach offers unique security advantages beyond what PPC profiles alone provide:

- Removes permissions granted before your security posture was hardened
- Ensures that even users who previously authorized Zoom can't be exploited
- When run every 15 minutes, creates an ongoing verification that no permissions exist
- Some organizations might prefer requiring users to explicitly re-authorize remote access for legitimate use cases, then having permissions automatically removed afterward

For security teams with diverse user populations, this represents a pragmatic middle ground. Rather than completely blocking remote control functionality (which might be occasionally necessary), the script allows temporary, conscious use of the feature while preventing persistent access that could be exploited between uses.

When permission removal events appear in your logs during normal operations, it's a strong indicator that either a user is attempting to use the remote control feature legitimately (requiring investigation and potential education) or that an attack attempt is underway. This visibility creates valuable security telemetry that helps identify both policy violations and potential attack attempts before they succeed.

Maximum protection by purging Zoom

For high-security environments or organizations handling cryptocurrency, the most direct approach is to completely remove Zoom from systems. This elimination strategy operates on a simple principle: software that isn't installed can't be exploited. For organizations handling particularly sensitive data or cryptocurrency transactions, the risk reduction from eliminating the Zoom client entirely often outweighs the minor inconvenience of using browser-based alternatives:

- Removes the application that ELUSIVE COMET relies on
- Ensures no remnant components remain that could be leveraged in an attack
- Removes all potential persistence mechanisms including preferences and cached data
- Guarantees that users cannot accidentally expose themselves to this risk

When combined with a policy encouraging browser-based meeting participation, purging zoom with `uninstall_zoom.bash` provides the strongest protection against ELUSIVE COMET's attack methodology.

Additional security recommendations

Beyond the specific Zoom mitigations, we recommend these additional defensive measures:

1. **Train users to recognize social engineering tactics in video calls:** While this is primarily a technical issue with Zoom's permissions model, user awareness still matters. Train staff to recognize unusual permission requests during video calls—particularly those requesting system control. Create a simple mental model for employees: “No legitimate business process should ever require giving someone else control of your computer.” Establish a protocol requiring secondary verification (like a phone call to IT) before granting remote control to anyone, even seemingly trusted contacts.
2. **Implement comprehensive IoC monitoring across communication channels:** Deploy email security tools like [Material Security](#) or [Sublime Security](#) that enable searching your entire organization for communications from known threat actors. When new indicators are published (like those in this post), these tools allow security teams to quickly identify if anyone in the organization has been targeted. Despite these attacks primarily occurring on social media, the attackers eventually need to send calendar invites via email—creating a detectable footprint if you have the right monitoring tools.
3. **Create explicit policies for media appearances and external communications:** At Trail of Bits, all media appearances follow an established process involving multiple stakeholders to develop messaging and talking points. When our CEO was approached via Twitter DM, his immediate response was to direct communication to email—following our standard procedure for external engagements. Establish clear verification processes requiring communication through official channels (corporate email) for any external engagement. Train staff that legitimate media organizations respect and follow these processes.
4. **Deploy email boundary controls as brand protection:** While this specific ELUSIVE COMET campaign didn't use email spoofing, properly configured DMARC, SPF, and DKIM prevent attackers from directly impersonating your domain in future campaigns. This limits an attacker's ability to exploit your organization's brand when targeting others. Bloomberg's properly implemented email security likely forced ELUSIVE COMET to use non-Bloomberg domains (gmail.com accounts)—a red flag that helped our CEO identify the attack immediately.
5. **Cultivate a rapid information sharing culture:** When our CEO identified this attack, he immediately posted a notification to the company-wide Slack channel, alerting everyone to the ongoing campaign. Create low-friction reporting channels that make it easy for employees to share suspicious interactions. Establish a “no penalty” culture for security reporting—reward people who report suspicious activity even if it turns out to be legitimate. Time is critical in these situations; a culture of rapid, blame-free reporting can prevent multiple victims within your organization.

Building resilient security against human-centered attacks

The ELUSIVE COMET campaign represents the continuing evolution of threats targeting operational security rather than technical vulnerabilities. As we've entered the era of operational security failures, organizations must evolve their defensive posture to address these human-centric attack vectors.

By implementing the multilayered defense approach outlined above, organizations can significantly reduce their exposure to this specific attack vector while maintaining business functionality. More importantly, this case study demonstrates the critical importance of combining technical controls with operational security awareness in defending against modern threats.

If your organization handles sensitive data or manages cryptocurrency transactions, our security engineers can help you develop a tailored threat model that addresses both traditional vulnerabilities and operational security boundaries. [Contact us](#) to learn more.