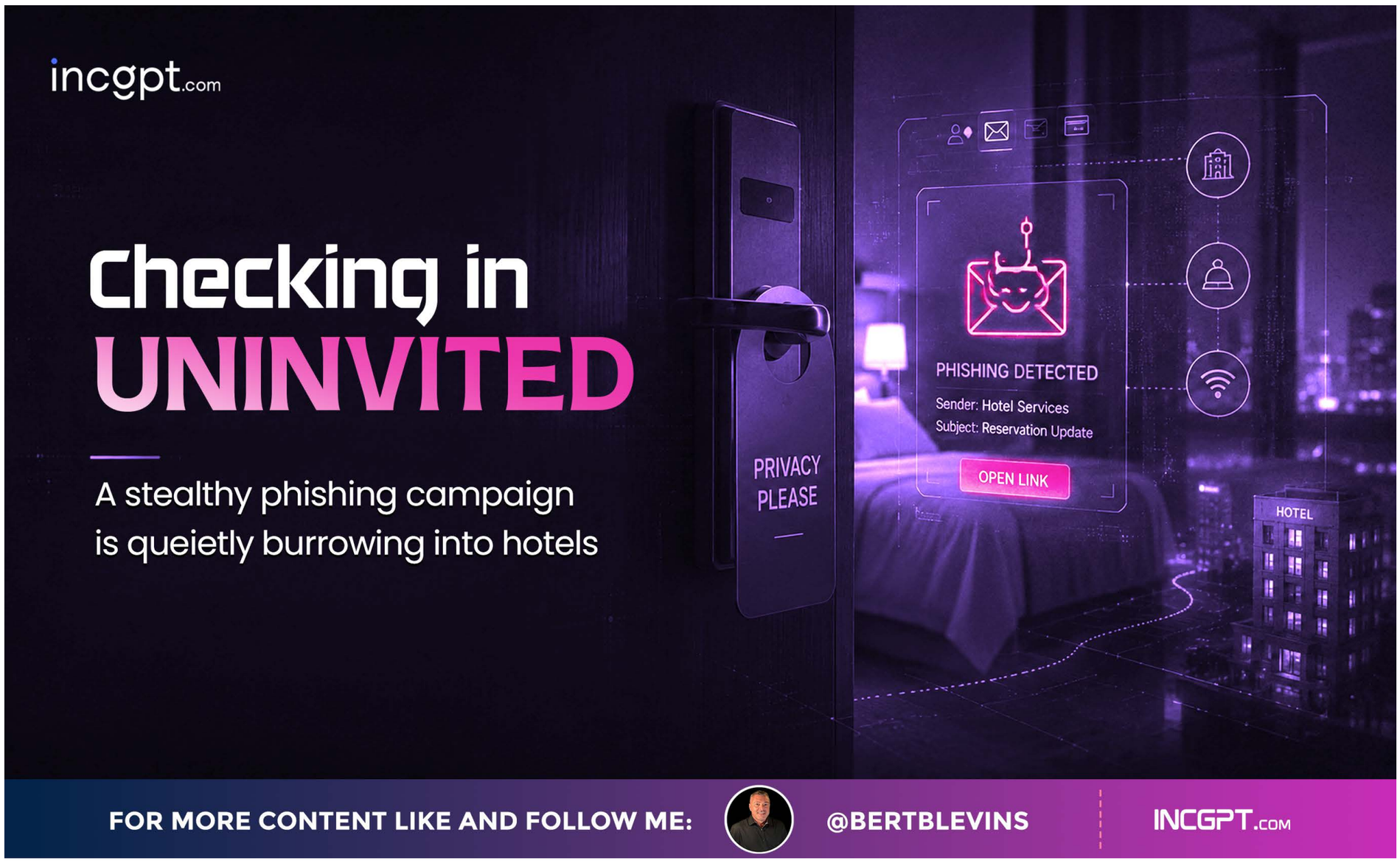
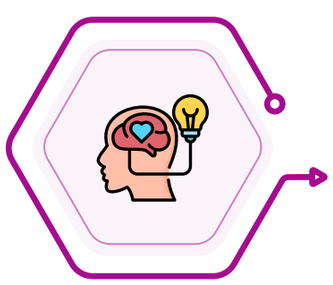
Checking In Uninvited:

A Stealthy Phishing Campaign Is Quietly Burrowing Into Hotels



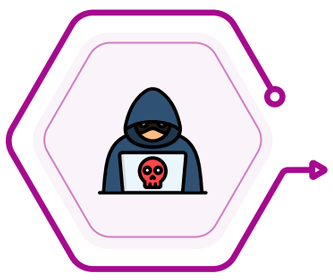
Someone is working hard to get a foothold inside hotels and hospitality companies across Europe and Asia, and the unsettling part is that no one yet knows exactly why. The activity has the look of careful groundwork rather than a smash-and-grab, which is precisely what makes it worth paying attention to.



According to Microsoft Threat Intelligence, which has been tracking the operation since April, an active phishing campaign is taking deliberate aim at the people most likely to open a stranger's message without a second thought: front desk, reception, and reservations staff. The lure is built around the everyday grind of hospitality work, with emails dressed up as guest complaints, room condition issues, bedbug reports, booking inquiries, and similar routine matters.

Why Hotel Front Desks Are the Perfect Target

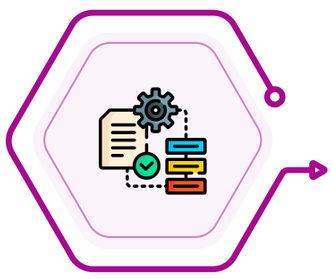
Reception teams exist to open messages from strangers. A complaint about a room or a question about a reservation is not a red flag to them; it is the job. That is exactly the instinct this campaign exploits. The messages arrive in multiple languages, including Danish, Dutch, and Japanese, tuned to the regions being hit so they read as ordinary correspondence rather than something suspicious.



The attackers are not blasting these emails out directly, either. They route them through legitimate services such as Calendly and Google's redirect infrastructure, a tactic that helps the messages sail past the standard email authentication checks of SPF, DKIM, and DMARC. Microsoft describes this as "authentication laundering": borrowing the trust of reputable platforms so a malicious message inherits a clean bill of health on its way to the inbox.

The Image That Isn't an Image

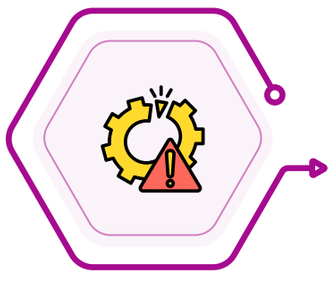
Once that laundering succeeds, the staff member receives a photo-themed ZIP archive, the kind of attachment that feels natural alongside a guest complaint. Inside, what appears to be a harmless picture file is actually a disguised shortcut file engineered to look like an ordinary image. Opening it does not show a photo. It quietly sets off a multi-stage infection chain that ends with a persistent implant built on Node.js taking up residence on the machine.



From there, the malware goes to work covering its tracks. It reconfigures Microsoft Defender to exclude itself, along with other randomly named files, from being scanned, pulls down additional payloads, and copies itself into multiple locations so it is harder to fully remove. The goal is persistence: staying put, staying quiet, and staying out of sight.

Reconnaissance, Not Yet the Main Event

On the systems it compromised, Microsoft watched the malware beacon out to its command-and-control infrastructure, gather environmental details such as the victim's public IP information, spin up hidden headless browser sessions, and in some cases force machines to shut down immediately. What it could not say is what all of this is ultimately for.



That uncertainty is the real story. Everything observed so far has the signature of a reconnaissance stage, the patient mapping of an environment that typically comes before something far more disruptive, such as a wider malware deployment or a ransomware strike. In other words, this may be the quiet phase before the loud one, which is why catching it now matters so much.

How Defenders Can Spot It

Because the operators lean on legitimate services and randomized file names, Microsoft advises organizations to hunt for the campaign's behavior rather than chasing individual indicators that can change from victim to victim. Security and IT teams in hospitality should watch for warning signs such as:

01 Photo-themed ZIP archives arriving with guest-complaint or booking-related messages.

02 Unusual PowerShell activity, including .NET compilation kicked off by PowerShell.

03 Unexpected Node.js execution running out of user profile directories.

04 Changes that add new exclusions to Microsoft Defender.

05 Random executables running from temporary folders.

06 Suspicious Run and RunOnce registry entries used to establish persistence.

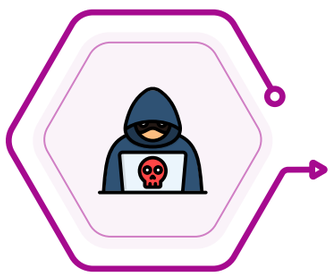
07 Outbound connections on the campaign's non-standard ports, and connections to newly registered .cfd domains.

08 Headless browser activity followed by sudden, forced shutdown commands.

Individually, several of these could be explained away. Seen together, they paint a recognizable picture, which is exactly why a behavior-led detection approach beats playing whack-a-mole with single indicator

The Takeaway for Hospitality

Hospitality runs on hospitality, on the willingness to engage with strangers quickly and helpfully. This campaign turns that strength into the attack surface, weaponizing the routine inbox of a reception desk to slip inside the network. The defense is not to make front-desk teams paranoid, but to pair their natural helpfulness with awareness: treat unexpected ZIP attachments with caution, verify unusual requests, and make sure security teams are watching for the behavioral fingerprints above.



No one knows yet what the attackers are planning. The smart move for any hotel or hospitality group is to assume the reconnaissance is real, find the foothold before it is used, and close the door while it is still just being tested.