# Scammers Weaponize Google Forms in New BazarCall Attack

hackread.com/scammers-weaponize-google-forms-bazarcall-attack/

December 13, 2023

Google Forms is the latest Google product to be abused by threat actors, this time for a new variant of the BazarCall attack

Cybersecurity researchers at Abnormal Security have identified a new attack campaign in which scammers use the **BazarCall technique (BazaCall or Callback phishing)** to target victims. This time, however, the notorious phishing attack method has taken a sophisticated turn by incorporating Google Forms to enhance its deceptive strategies.

Here, it is worth noting that Abnormal Security's findings came just a couple of weeks after the **FBI warned users** of the Silent Ransom Group (SRG), also identified as Luna Moth, employing Callback phishing techniques for network hacks.

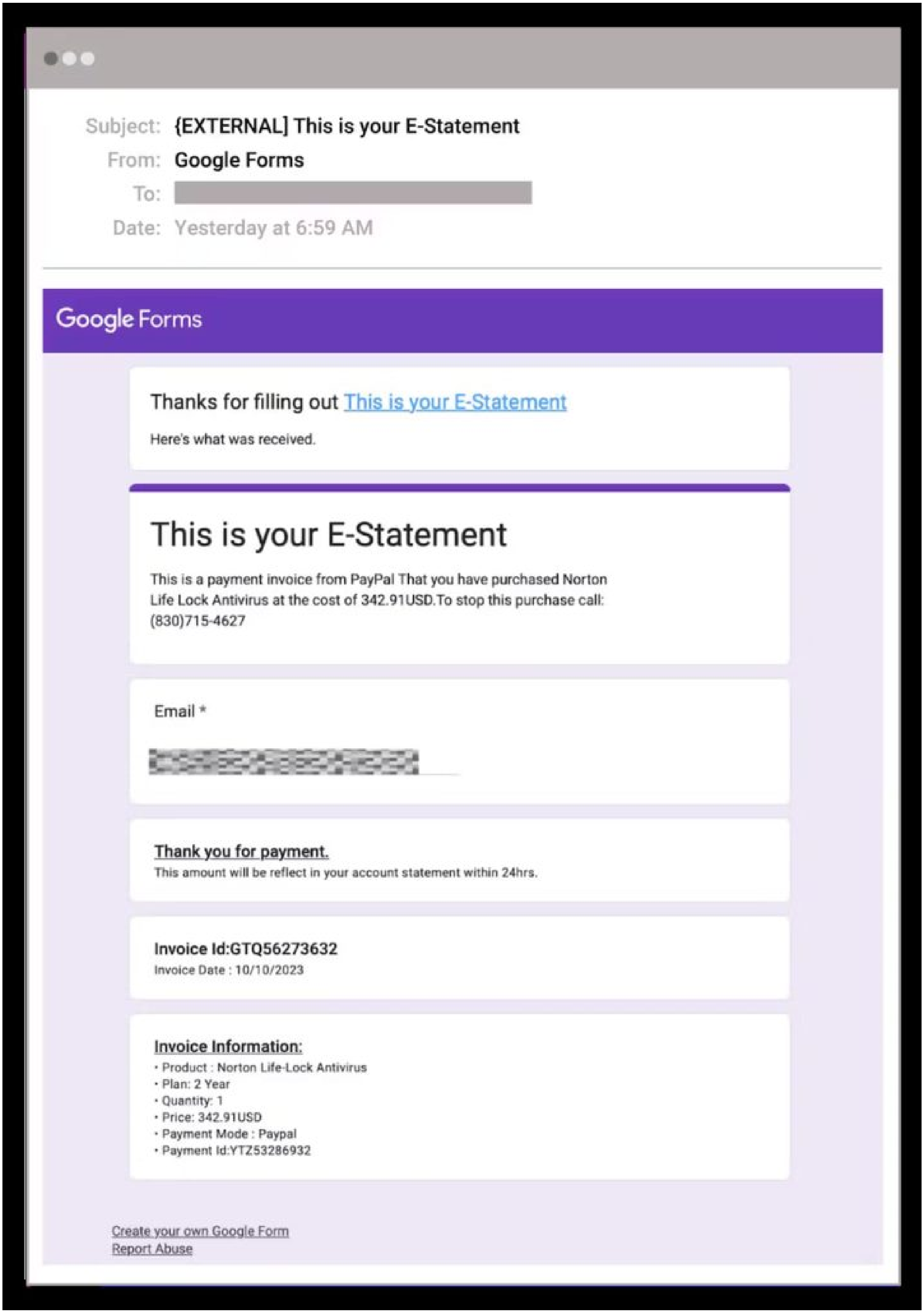
In the usual scenario, the BazarCall attack typically begins with a phishing email masquerading as a payment notification or subscription confirmation from familiar brands. The email prompts recipients to call a provided phone number to dispute charges or cancel a service, creating a sense of urgency. However, the real objective is to **trick victims into installing malware** during the phone call, exposing organizations to future cyber threats.

What sets this BazarCall variant apart is its utilization of Google Forms to elevate the authenticity of malicious emails. The attacker crafts a Google Form, adding details about a fake transaction, including an invoice number and payment information. The response receipt option is then activated, sending a copy of the completed form to the target's email address.

In a **blog post**, Mike Britton Chief Information Security Officer at Abnormal Security, said that the attacker manipulates the process further by sending the form invitation to themselves, completing it with the target's email address, and making it look like a payment confirmation for a product or service. Using Google Forms, sent from a legitimate Google address, enhances the attack's legitimacy, making it harder to detect.

> *"Because the email is sent directly from Google Forms, the sender address is forms-receipts-noreply@googlecom, and the sender display name is "Google Forms." Not only does this contribute to the appearance of legitimacy, it increases the chances of the message being successfully delivered as the email is from a legitimate and trusted domain."*
>
> *Mike Britton – Abnormal Security*

The uniqueness of this BazarCall lies in its difficulty to be identified by traditional email security tools. Unlike typical threats with malicious links or attachments, this attack relies on Google Forms, a trusted service for surveys and quizzes.



Subject: {EXTERNAL] This is your E-Statement

From: Google Forms

To: [redacted]

Date: Yesterday at 6:59 AM

Thanks for filling out This is your E-Statement

Here's what was received.

## This is your E-Statement

This is a payment invoice from PayPal That you have purchased Norton Life Lock Antivirus at the cost of 342.91USD.To stop this purchase call: (830)715-4627

Email *

[redacted]

**Thank you for payment.**

This amount will be reflect in your account statement within 24hrs.

**Invoice Id:GTQ56273632**

Invoice Date : 10/10/2023

**Invoice Information:**

- Product : Norton Life-Lock Antivirus
- Plan: 2 Year
- Quantity: 1
- Price: 342.91USD
- Payment Mode : Paypal
- Payment Id:YTZ53286932

Create your own Google Form

Report Abuse

Actual email sent by threat actors using Google Forms (Image credit: Abnormal Security)

Actual email sent by threat actors using Google Forms (Image credit: Abnormal Security)
The dynamic nature of Google Forms URLs further complicates detection, as they frequently change, evading static analysis and signature-based detection used by many security tools. Mike further noted that legacy email security tools, such as secure email gateways (SEGs), struggle to discern the malicious intent behind these emails, leading to potential threats slipping through the cracks.

However, modern **AI-native email security solutions** with behavioural AI and content analysis can accurately identify and thwart such attacks by recognizing brand impersonation and phishing attempts.

In a statement to Hackread.com, Google confirmed its awareness of a newly emerging, yet isolated, phishing campaign utilizing Forms.

> *"Workspace has numerous layers of defences to keep users safe. We are aware of the recent phishing attacks using Forms, and while they appear to be isolated to a small number of users, we are working to improve detection."*
>
> *A Google spokesperson*

Nevertheless, in navigating the evolving cyber threats, staying informed about sophisticated attack methods like this BazarCall variant is crucial. Adopting advanced email security solutions that leverage artificial intelligence is paramount to effectively protect organizations and individuals from the ever-changing tactics of cybercriminals.

## *RELATED ARTICLES*

1. **New BEC 3.0 Attack Exploiting Dropbox for Phishing**
2. **Phishers Exploiting Google Docs to Harvest Crypto Credentials**
3. **Iran's MuddyWater Group Targets Israelis with Fake Memo Phishing**
4. **USPS Delivery Phishing Scam Exploits SaaS Providers to Steal Data**
5. **Hotel booking phishing scam uses PDF links to spread MrAnon Stealer**