Intigriti insights into latest beg bounty scam

BY ELEANOR BARLOW · MARCH 25, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **What "beg bounty" scams are and how malicious actors exploit bug bounty systems** by submitting fabricated or manipulated findings to demand payment.
- **How these scams can impact businesses, especially SMEs without formal bug bounty programs,** and why proper triage and verification are critical to distinguishing fraud from legitimate security reports.
- **How reputable bug bounty platforms and expert triage teams help protect organizations by filtering out fraudulent activity** and ensuring only credible security research leads to actionable insights and rewards.

The Intigriti team have recently observed an abuse scenario, trending across the industry, where malicious actors are posing as legitimate white-hat hackers, deceiving targeted companies into believing their actions are carried out in good faith.

> **"Bad actors will always try to exploit the system, in any industry, for personal gain. At Intigriti, we help customers navigate this landscape by ensuring only legitimate security research makes it through. Our expert triage team identifies and filters out fraudulent reports and actions, allowing businesses to focus on real threats and on enhancing their security posture with confidence."**
>
> **Inti De Ceukelaire, Chief Hacker Officer, Intigriti**

How the beg bounty scam works

While white-hat hackers can be invaluable when employed properly, problems arise when hackers lack proper verification and credibility.

Coined 'beg bounty' hunting, scammers collect and upload seemingly sensitive documents to the targeted apps and platforms, only then to report this data as leaked or vulnerable on their systems. The goal is to demand a bounty for identifying the "issue".

Beg bounty use case explored

Recently, the Intigriti team observed a user execute the following actions.

1. The bad actor tracked targets with online helpdesk software that was available without authentication.
2. The user then submitted a ticket with an attachment of sensitive data. This can, for instance, include scans of Personally Identifiable Information (PII), such as images of passports. Since the helpdesk was

available without authentication, the attachments were too.

3. The user then self-submitted the exact URL for the attachment to VirusTotal and then submitted the 'leaking' of this attachment as a security concern for the company.

4. Finally, the user submitted a payment request for identifying the ‘threat’.

> **“As a triage team working for many customers, we’re quick to observe trends, using knowledge gained from triaging one customer report to help our entire client base. This way we gain insights and spot issues internal teams might miss. ”**
>
> **Lennaert Oudshoorn, Head of Triage, Intigriti**

Multiple forms of beg bounty scams targeting businesses

Another form of beg bounty hunting occurs when ‘bounty beggars’ request payment before revealing a ‘vulnerability’ to a company, only to highlight an issue that is not considered a threat or vulnerability, and thus not deemed worthy of payment. Their focus is on quantity over quality, regardless of value to the customer. Rather than fabricating a data leak or vulnerability, here the actor searches for low-hanging fruit and then demands payment before releasing the data. While reporting minor issues is accepted and appreciated within the industry, the issue is the cajoling of payment.

Beg bounty scams preventing necessary actions

These types of threats have been circulating for many years and cost businesses dearly. In 2017, Troy Hunt released a blog discussing the serious privacy and security issues surrounding the company, CloudPets, which manufactured internet-connected soft toys. The blog showcased an incident regarding an internet-connected toy teddy bear that allowed parents to send voice messages to their children. Due to a publicly accessible and unprotected MongoDB database, 2.18 million voice recordings and 820,000 user records were exposed.

What makes this data breach so alarming is that multiple attempts were made by security researchers to warn CloudPets about the vulnerability. Yet the company failed to respond. The reason? CloudPets did not trust the information of a random person but equally did not undertake due diligence to check that the information was accurate.

In a statement by CloudPets CEO, Michael Kan claims that ‘We did have a reporter try to contact us multiple times last week, you don't respond to some random person about a data breach.’

The issue here is that if your internal or third-party security teams have not spotted the issue, the only people who are going to spot vulnerabilities like this are bug bounty hunters and well-intended reporters, who should not be ignored. When a company is notified of a threat, it falls to the diligence of the company to do its homework on what is being reported, especially when multiple notifications have been sent regarding such a sensitive subject matter.

Beg bounty scams are instilling a culture of fear and muddying the water for legitimate white-hat hackers and reporters.

Who is targeted?

Small to Medium Enterprises (SMEs) without legitimate bug bounty programs in place are at greater risk. SMEs not only have limited resources but often lack efficient funding for additional cyber security, which makes it easier for hackers to circumnavigate environments.

Although there are few statistics to support the growth of beg bounty schemes specifically, the tactic contributes to the overall landscape of cybercrime and cyber fraud. In a report provided by the Global Anti-Scam Alliances 2024, UK residents alone lost £11.4 billion to scams in a single year, a number that has risen by 4 billion since 2023.

The importance of triage to spot fraudulent activity

The key message is for businesses to utilize reputable companies. Legitimate bug bounty teams stay on top of the most recent developments, tactics and procedures, and work on a wide range of programs to spot trends and information that an internal team would usually miss.

It takes a high-level verified hacker with the right skill set to spot actual system issues that would impact the security of a company. Often low-level hackers will try and spot and report anything, regardless of impact.

By having a bug bounty plan in place, companies benefit in multiple ways:

1. Guesswork is removed on who or what to trust.
2. The client's time is saved by having a team to investigate and close reports.
3. Users are validated so you know exactly who you are working with.
4. An expert team monitors all actions and closes all reports before any payment is made.
5. Ability to ban users from platforms for unethical actions.

For more information on how bug bounty works, and how to spot bogus beg bounty schemes, contact the Intigriti team, today.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.