LY FORENSICS

ANALYSING SCAMS

INVESTIGATION OF A SEXTORTION SCAM

DATE:
19 Dec 2024

WRITTEN BY :
Lawrence Meckan

1300 168 380 Option 4
lyforensics.com.au

Report Objective

This report was created to raise awareness of sextortion scams using cryptocurrency being spread online.

It details the steps our team took to investigate the targeted sextortion attempts and presents our findings. No exploitation was performed, only reconnaissance of publicly available attributes and entities including the enumeration of the scammer's email content and headers.

Please note that this is a real scenario and is intended for educational purposes only. It demonstrates what these scams look like and how they operate based on observations. Use this report solely for learning and understanding how to stay safe from such scams.

During this investigation, our team utilised a secure, external Virtual Machine to conduct all testing. Best practices and security procedures were strictly followed and thoroughly verified upon completion.

Please also note throughout this report, we make mention of SendGrid, Binance and Paxful. These companies are legitimate and are **NOT** tied to this scam.

Scam Initiation

Multiple clients have received emails claiming that they had been hacked.

The emails claimed to be from a hacker who said they had gained unauthorised access to the client's operating system and account.

They made claims to have been monitoring the client for several months after allegedly infecting their device with malware from adult websites.

The hacker:

- Claimed to have full access to the client's device and account
- Said they can view the screen, camera, and microphone remotely
- Threatened to share compromising video footage unless paid between $500 and $1,500 in cryptocurrency
- Gave a 2 day deadline to comply
- Warned against reporting the incident or sharing the email
- Provided a randomly generated image of a blurred-out male as an attachment

These emails may come from multiple sources, either legitimate business domains or mail provider services such as SendGrid.

These emails appear to be classic examples of a sextortion scam, attempting to extort money by threatening to reveal embarrassing information. Such scams typically rely on duress rather than actual access to devices or compromising material.

Now we have identified the emails as suspicious, let's dive deeper into how this scam aims to get the victim's funds.

Down the Rabbit Hole

The sextortion scam works primarily by sending the same threat at scale. It is for this reason third-party mail provider services such as SendGrid are used. Where other legitimate domains are used, open source intelligence (OSINT) on them shows they are being exploited through their mail servers. These mail servers were insecure in their configuration.

We analysed multiple sextortion emails from clients. We did this to form a representative sampling of similarities and differences between each attempt at sextortion. This allowed us to understand the financial clustering and cryptocurrency strategies behind such a scam.

The primary targets of this sextortion email were shown to be:

- Young males, either in teens or young adulthood, with little social media training or experience
- Older males with either established families or from non-traditional upbringing

The targeting we found was aimed to elicit an immediate response to bring the victims into the scam. The examples shown above demonstrate family life and social structures may be seen as a threat vector, which the scammers then aim to exploit

This is why on some sextortion emails provided to us we saw a blurred image of a male implied to be on a webcam as an attachment. The scammers were attempting to provide social proof when it was not legitimate.

We have analysed 3 provided cryptocurrency addresses used in the sextortion scam emails provided. Whilst they are not all the cryptocurrency wallets provided to us, they help build a test sample. For due disclosure purposes of our clients, we are not publishing them all.

The wallet address we are investigating are:

- A Bitcoin address: 3E5tqtwsAF9A8pbdBSFgifRrotnBAr6dBR3E5tqtwsAF9A8pbdBSFgifRrotnBAr6dBR
- A second Bitcoin address: 1KfDSTkha7VFhXthkrBQz1NU5neYA5KZ2W
- A Tron (TRC-20) address: TDxUkUVW8bYtkQyK1GjbhrCBe5Sovxj55M

Forensic track and tracing analysis of these supplied cryptocurrency addresses found offramps to legitimate cryptocurrency exchange providers such as Paxful & Binance. Both Binance and Paxful remain regulated cryptocurrency exchange providers in their relevant jurisdictions. The transaction amounts were below worldwide anti-money laundering (AML) and financial crime thresholds.

This told us there were, on average, 8 people who responded to each sextortion scam when it was sent out.

Email messaging provider services generally have a low open rate, leading to low conversion rates as part of online commerce. The blockchain analysis of the cryptocurrency addresses listed in the sextortion emails provided by our clients matches this low conversion rate.

We can ascertain the scammers aim to maximise return on their investment by rotation of cryptocurrency addresses in each sextortion scam with a monetary amount that may not raise suspicion. Potential victims may be sent multiple sextortion emails covering multiple cryptocurrency addresses. This shows the scammers aim to social engineer shame and guilt through extortion.

By rotating the cryptocurrency wallets used in these sextortion spam emails, the scammers aim to lower the risk of any forensic investigation of their behaviour and tactics, as the monetary loss by each victim is significantly lower than any AML or financial crime thresholds set worldwide

Conclusion

The investigation into these sextortion emails has provided valuable insight into how these types of scams operate. By diving into the various elements of the scam, such as the services used and cryptocurrency addresses, our team was able to uncover the methods these attackers use to manipulate unsuspecting users. This report outlines the basic steps and techniques used in this extortion attempt, showing the processes that occur at face value.

One crucial aspect of the investigation was identifying and analysing the cryptocurrency addresses supplied in these sextortion emails. These cryptocurrency addresses, much like the use of email marketing services and exploiting other commercial email providers, are readily spun up, used and then recycled for a new cryptocurrency address in the next sextortion spam email.

The aim is to get a quick return on the investment through exploiting people's vulnerabilities and fears with social engineering. Once the victims have been exploited, the scammers then offramp their funds to legitimate cryptocurrency exchanges.

This shows sextortion scams run primarily by distributing the scammer's risk via cryptocurrency wallet rotation and the ability to send out unique wallet addresses at scale with email provider services.

Platforms like SendGrid are also being exploited. Scammers can easily create email lists under false pretences and use them to distribute extortion emails to large groups of potential victims. This serves as a reminder that even seemingly legitimate services can be misused by malicious actors, which is why it's important to be cautious when receiving unsolicited emails or messages, even if they appear to come from trusted sources.

Throughout this investigation, we utilised various tools and methods, such as Shodan for IP address analysis and OSINT wallet analysis, to dig deeper into the scam's infrastructure. By reviewing the email infrastructure along with the cryptocurrency addresses, we were able to understand the specific actions the scam was designed to carry out throughout this process. This level of detail is necessary to comprehend the full scope of the attack and provide actionable insights for others to avoid falling victim to similar scams.

This investigation was not intended to provide a deep technical analysis, but rather to give a foundational understanding of a real, ongoing scam. The tactics used here, such as social engineering, and the use of reputable platforms for malicious purposes are all part of the evolving landscape of cybercrime. By being aware of these methods and understanding the behaviours of scammers, you can better protect yourself from falling prey to similar scams in the future.

At the time of publication, the specific sextortion campaign described in this report is no longer active. However, similar scams remain prevalent and continue to target users.

LY Forensics strongly recommends maintaining vigilance when receiving unsolicited emails seeking to extort funds from you or those you know.