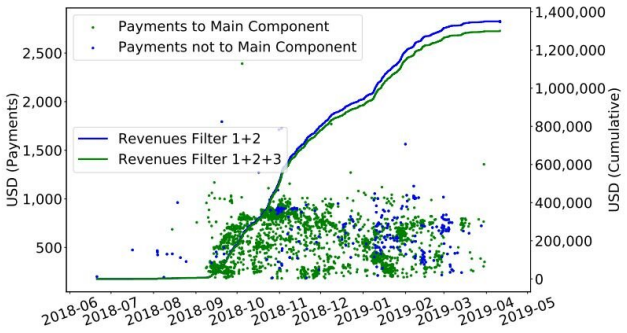
Sextortion shakedown attempts for Bitcoin payoffs get full anatomy

20 August 2019, by Nancy Cohen



Sextortion's cumulative revenues combining di erent lters and single payments to sextortion addresses. Credit: arXiv:1908.01051 [cs.CR] https://arxiv.org/abs/1908.01051

For the uninitiated, the word Bitcoin summons up a mixed emotion of approach-avoidance. It teases curiosity to know more about this fascinating alternative to conventional currency and at the same triggers unease about its bad reputation. New research is not likely to make the approach-avoidance crowd take a leap of faith.

"Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem" by Masarah Paquet-Clouston, Matteo Romiti, Bernhard Haslhofer and Thomas Charvat, submitted on August 2, is now up on arXiv.

The sextortion to which the authors refer has to do with a scam campaign that made the rounds in 2018 and caught the attention of CBS News back in July 2018. "Using stolen passwords to get a victim's attention, a new sexploitation scam threatens victims with exposing them "doing nasty things." In an emailed threat, the crook claims to have downloaded malware on the victim's computer that enabled the crook to take over the victim's webcam."

Then the scammers turned up the screws in saying they had a list of the potential victim's contacts and planned to tell all if not sent a payoff.

"The crook also claims to have pilfered email and social media contacts and to have a recording of the victim, filmed from the victim's own webcam, watching porn. Demanding a ransom in bitcoin, the scammer says if the victim doesn't send $1,000 to $2,000 within 24 hours, the crook will share compromising images of the victim with all of the victim's contacts."

This scam got a heads-up, too, back in February when Christopher Boyd, a malware intelligence analyst, said in *Malwarebytes* that a "particularly nasty" sextortion scam from at least the middle of 2018 was making the rounds again.

Then what is news about this latest research on arXiv? The value is that it is a detailed anatomy of how this type of campaign works, succeeds, and, in the words of *MIT Technology Review*, "just how much money this type of scam can generate."

(Noted in *MIT Technology Review*: "Various researchers have shown that spammers pay botnet owners between $100 and $500 to send a million spam emails. They can even rent botnets at a cost of $10,000 per month, which allows them to send 100 million spam messages.")

How did the authors pull apart the method used by sextortion spammers? They said they dove into a dataset of 4,340,736 emails related to sextortion, identifying different threat campaigns and evaluating pricing strategy. Then, they extracted Bitcoin addresses and investigated transactions related to sextortion in the Bitcoin ecosystem.

Tools? They used open-source GraphSense Cryptocurrency Analytics Platform1, projected onto transaction graphs by applying the "multiple-input clustering heuristic." They estimated spammers'

potential revenue through different techniques and also analyzed patterns in monetary flows.

The researchers examined a lucrative 11-month operation cutting "the upper tail of the spamming supply chain." The operation yielded between $1,300,620 and $1,352,266.

Conclusions? "These folks have studied a huge data set of sextortion emails to better understand how this kind of scam works. Their worrying conclusion is that it is lucrative and likely to become more widespread, said *MIT Technology Review*.

The researchers said in their paper that spammers will likely continue sending out bulk emails trying to extort money through cryptocurrencies.

Back in April, Ethan Sidelsky asked, "Why Do Cryptocurrencies Have Such a Bad Reputation?

In *Medium*: "For most people, cryptocurrencies have mainly negative associations—words like scam and bubble often come to mind. The reason for this is that the coverage of cryptocurrencies by the mainstream media has largely been negative—not without reason," he wrote. What shook the boat? "While there are lots of great projects being built in the cryptocurrency community, there are also lots of scams and criminal activity." He added that cryptocurrencies are often used for illegal payments, such as buying drugs or fake ID's, because they are anonymous and decentralized.

More information: Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem, arXiv:1908.01051 [cs.CR]
arxiv.org/abs/1908.01051

APA citation: Sextortion shakedown attempts for Bitcoin payoffs get full anatomy (2019, August 20) retrieved 26 May 2022 from https://techxplore.com/news/2019-08-sextortion-shakedown-bitcoin-payoffs-full.html