Decentralized Cryptographic Information Black Market

Jean-Loup Richet

Abstract:
This article highlights a new business appeared on the cybercrime underworld: a decentralized and anonymous black-market in which one can sell any confidential and valuable information. What is promoted as a platform for whistleblowers is in fact a place where one could sell stolen credit cards data, 0 day exploits and software vulnerabilities, child porn, stolen databases, and so on and so forth. We describe the mechanisms of this platform for cybercriminals, explain its fallacy, and argue for the need of protection for real 'moral heroes' - individuals protecting our human rights and pushing back against corruption and state powers.

Keywords:
whistleblower, cybercrime, bitcoin, cryptographic, black-market, information marketplace.

Buy and Sell data leaks anonymously

I have recently discovered Darkleaks, a decentralized and anonymous black-market in which you can sell any confidential and valuable information.

The service advertised all over the internet with a sales speech like this:
Do you want to be a whistleblower - or do you want to make a few bucks out of data leaks? Have you ever dreamed of distributing an encrypted data leak to the world, let people bid on this dark secret, and earn money anonymously through bitcoin?

Project's developers promote it as:

> The best tool to trade any kind of media, information, video, data and documents that have value.
> > Hollywood movie
> > Trade secrets
> > Government secrets
> > Proprietary source code
> > Industrial designs like medicine or defense
> > Zero day exploits
> > Stolen databases
> > Proof of tax evasion
> > Military intelligence
> > Celebrity sex pictures
> > Corruption

How does it work?

When the leaker selects a document, it is broken up into segments. Each of the segments is hashed, and a Bitcoin address is generated using the hash as the secret key. From this public key, a new key is generated to encrypt the segments. The encrypted segments are released for public download with the list of Bitcoin addresses.

To prove the authenticity of the document, the system uses a trustless provably fair mechanism. When announcing the leak, the leaker chooses a date and number of the chunks to be released. Based on the Bitcoin block hash at that time, some provably fair random numbers are chosen to select segments to be unlocked. This allows the community to verify the veracity of the file and decide whether they want to pay for the remaining encrypted segments.

The buyers then send Bitcoins to these addresses. When the leaker decides to claim the Bitcoins from the private key, due to how Bitcoin is designed he must release the public key which allows the buyers to decrypt the document.

Because the leaker cannot pre-choose which segments are released, the buyers can verify the addresses are correct, and the segments can be decrypted. This makes for an authenticable and trustless mechanism for selling information on the decentralized black market.

We need to protect 'moral heroes'... not another cybercriminal underground marketplace

Of course, we need individuals to protect our human rights and push back against corruption and state powers – and we need to protect these individuals.
After the whistle, most leakers of government secrets have their lives changed. Sentencing in media leak cases has historically been relatively light from 1973 to 2005, with only 24 months of prison time for the three whistleblowers prosecuted. Yet, ACLU observed that Obama has "*secured 526 months of prison time for national security leakers,*" with the vast majority given to Chelsea Manning, who was sentenced to 35 years.
Edward Snowden, former NSA employee who released classified documents on U.S. monitoring plans is now in Russia, with his destiny at stake. The Justice Department declared mid 2013 that it won't seek the death penalty in prosecuting him, but he is still charged with thievery and espionage.

However, in the case of Darkleaks, I fear that this platform will also be an area where one could sell stolen credit cards data, 0 day exploits and software vulnerabilities, child porn, stolen databases, and so on and so forth. Indeed, there is a huge market for personal data, from US SSN to email addresses through credit cards data (Acquisti, Taylor, & Wagman, 2014). This black market will soon be overcrowded with scammers - no crystal ball is required to predict that it will become a future playground for cybercriminals…

Could we compare Darkleaks market model with software vulnerabilities markets?
On this very topic, I really liked Kannan & Telang (2005) research on software vulnerability disclosure markets. The authors demonstrate that an active unregulated market-based mechanism for vulnerabilities almost always underperforms a passive infomediary-type mechanism.
To sum up, a movement toward a market-based mechanism might not lead to a better social outcome…

The issue of anonymity remains. Whistleblower Protection Acts are a false hope. According to Martin (2003), they are just an appearance of protection: remarkably inefficient, flawed and unhelpful. **How to protect 'moral heroes' (Malin, 1982)?**

Syta, Michael and Ford (2014) might have the solution – their convincing research pitch is as follows:

"In privacy-sensitive communications, one user sometimes needs to prove to be a member of some explicit, well-defined group, without revealing his individual identity.

Consider for example a whistleblower who wishes to leak evidence of corporate or government wrongdoing to a journalist, via an anonymous electronic "drop box".

The journalist needs to validate the source's trustworthiness, but the whistleblower is reluctant to reveal his identity for fear their communications might be compromised, or that the journalist will be coerced into testifying against the source.

The whistleblower thus wishes to authenticate anonymously as a member of some authoritative circle who plausibly has knowledge of and access to the leaked information, such as a corporate board member or executive, or a government official of a given rank.

Even if the whistleblower convinces the journalist of his authority, the journalist may also require corroboration: e.g., confirmation by one or more other members of this authoritative circle that the leaked information is genuine. Other members of this authoritative circle may be just as reluctant to communicate with the journalist, however. If a potential corroborator also demands anonymity, how can the journalist (or the public) know that the corroborator is indeed a second independent source, and not just the original source wearing a second guise?

In general, if the journalist knows k pseudonymous group members, how can he know that these pseudonyms proportionally represent k real, distinct group members, and are not just k Sybil identities?

Finally, the whistleblower is concerned that once the leak becomes public, he may be placed under suspicion and any of his computing devices may be confiscated or compromised along with his private keys.

Even if his keys are compromised, the whistleblower needs his anonymity forward protected, against both the journalist and any third-parties who might have observed their communications. Further, the whistleblower wishes to be able to deny having even participated in any sensitive communication, including the fact of having authenticated at all (even anonymously) to the journalist."

Syta, Michael and Ford (2014) protocol satisfy the above requirements (anonymity, proportionality, forward anonymity, and deniability). Their research paper might be an interesting reading for journalists and wannabe moral heroes waiting to uncover corruption and wrongdoing.

References:

Acquisti, A., Taylor, C., & Wagman, L. (2014). The economics of privacy. *Journal of Economic Literature*.

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science*, *51*(5), 726-740.

Malin, M. H. (1982). Protecting the Whistleblower from Retaliatory Discharge. *U. Mich. jL Reform*, *16*, 277.

Martin, B. (2003). Illusions of whistleblower protection. *UTS L. Rev.*, *5*, 119.

Syta, E., Michael, B. P. D. I. W., & Ford, F. B. (2014). Deniable Anonymous Group Authentication. Retrieved from cpsc.yale.edu

***

Blog post from https://blogs.law.harvard.edu/jeanlouprichet/