

Forum:[Hack Forums](#)

Thread: [Social engineering as a method of obtaining an entry point into a corporate network](#)

vasper - June 23, 2025, 10:53 am

I decided to write this article as a brief overview of the methods known to me. All the tools I listed are debugged and have repeatedly brought results to both me and my partners. I based the article on the text that I used at a closed conference organized for droppers from several forums known to you. I made a minimum of changes to the text, since I am addressing the owners of drop projects. I hope that my article will be of interest and will allow you to look at your usual activity from a new angle. Over the past few years, colossal volumes of big data have passed through us, during the audit I always have to deal with the analysis of mail files, ranging from Outlook (.msg) to cutting up heavy PST arrays containing internal corporate correspondence between employees. In absolutely every company I encounter violations, including corporate ethics. Middle and lower level employees constantly complain about working conditions, low wages, racial and gender discrimination, sexual harassment in the workplace, career stagnation, endless penalties from senior management, etc. Often, there are records of corporate psychologists from which it follows that the vast majority of personnel feel oppressed and undervalued. Moreover, all this applies to both small companies and those with a profit of several billion USD. What is this if not a tool of social engineering influence?! Surely many of them thought about how to take revenge on their bosses or get a part of the superprofits that they observe from year to year working in their organization, but to which they have nothing to do. Of course, there is no need to have illusions about recruiting top management, their inflated bonuses and premiums speak for themselves. Do not forget that we are not necessarily interested in current employees, these can be people with family ties or acquaintances, those persons who can offer so-called assistance. Industrial espionage has existed for many years before you and I were born and will always exist. The entire Western business model is imbued with greed, just as corruption, envy and other "benefactors" are not alien to them anywhere.

Moreover, it is necessary to understand all the strict rules of capitalist society, the legal system together with government agencies and banks have long created conditions under which you have no right to stumble.

Option #1: Partial reorganization of the drop project. As far as I know, it is not uncommon for a new drop to immediately say upon registration that he understands the whole point. You can start a direct dialogue with such people. It is not because of a good life that they go to receive wire/ach or carzhen staff with forwarding, as a rule, they have a main job and do not suspect that they can be useful for more serious tasks. All that is needed is for your drop to have access to any of the organization's computers. Starting from storekeepers, packers, sellers and administrators, ending with the reception of a hotel or restaurant, almost every workplace in the US and EU is computerized and automated. Perhaps it is obvious to some of you, but for understanding the technical side, it is not superfluous to remind you that even the most remote machine belonging to a corporate network, located in a demilitarized zone or in a trust domain, can serve as a high-quality, primary access point for launching an attack on the entire network. Everything rests on the liquidity of the company and the skills of the pentester. On the basis of an already prepared drop project, you can conduct a survey among both already registered "adepts" and newcomers, the purpose of which is to find out where a person currently works and whether he has close friends or relatives in large companies. As practice shows, it does not take long to persuade someone to cooperate; if a person deliberately goes for banking fraud, I assure him that your offer will be very interesting. To intrigue, a pre-prepared text containing security instructions and examples with high-profile cases will be enough. Having googled several articles that focus on the amounts and impunity of attackers, their greed will do the lion's share of the work for you.

Option #2: A dedicated project without disguise.

This involves creating a resource on an onion domain (or on a bulletproof hosting) for an open offer.

The promotion of such a resource can be carried out through banal spam, posts on social networks or targeted mailings to company employees on LinkedIn, etc. Particular attention should be paid to X (aka Twitter) and Reddit. At the moment, their accounts, including pumped up ones with a huge number of subscribers, can really be bought for modest amounts. Antifraud is minimal (login + pwd + cookies), it is very easy to get in and most importantly, on the above-mentioned social networks there is a huge number of info gypsies and communities dedicated to stock market trading, analytics and finance. Mommy's investors graze there in crowds waiting for hype like GameStop. Ideally, this option should promote itself after some time by word of mouth. It all comes down to a well-prepared information bomb in social networks. The primary message should be capacious, not compromise, but simply lead a person to the site for review. The <Home> page sets out in detail the essence of the matter, be it stock exchange insider information, theft of developments or ransom with examples of cases and the amounts that can actually be obtained. Such examples can be many articles on each of the topics, of which there are more than enough on the Internet. For clarity and ease of understanding, create a video for YouTube demonstrating how it works with a voiceover. In another subsection of the site, it is supposed to enter data: the name of the company in which it works (has access) and data for feedback, for example, qTox, jabber, telegram. It is also possible to have feedback directly on the site itself, in the form of an onion chat. It would not be superfluous to place links to articles on the confidentiality of using these messengers, as well as safety instructions that include such key points as:

- do not contact us from your corporate workplace
- use a prepaid SIM and a device purchased for cash
- detailed instructions on registering jabber and setting up PGP/OTR

All these points say - "we care about your privacy and security", which in turn will dispose them to the resource.

Option #3: Personal blackmail.

A few years ago, a blackmail scheme for small amounts was popular. After familiarizing themselves with a mailbox or a social network account, the owner received a message with ransom demands, under the threat of distributing intimate photos and other compromising data among friends and colleagues. It is likely that instead of \$ 500 in ransom, the victim will agree to run malicious code or execute a powershell command on one of the corporate machines. Do not underestimate the determination and capabilities of people driven into a corner, when their reputation or personal life is at risk, especially when it comes to the female gender. In this case, it is necessary to implement an automatic search by keywords inside the mailbox and social networks of compromising materials. In fact, industrial or state espionage involving women is an eternal classic, the question rests only on motivation, in our case, on pressure. The recent scandal with Puff Daddy is a clear confirmation of this: one person, with the help of blackmail, maintained control over the entire media industry and successfully benefited from it for many years.

In conclusion, I would like to add that if you or your partners have experience with any of the above options, I would be grateful if you write to me in PM, while I draw your attention to the fact that at the moment we are working very fruitfully on option #2.