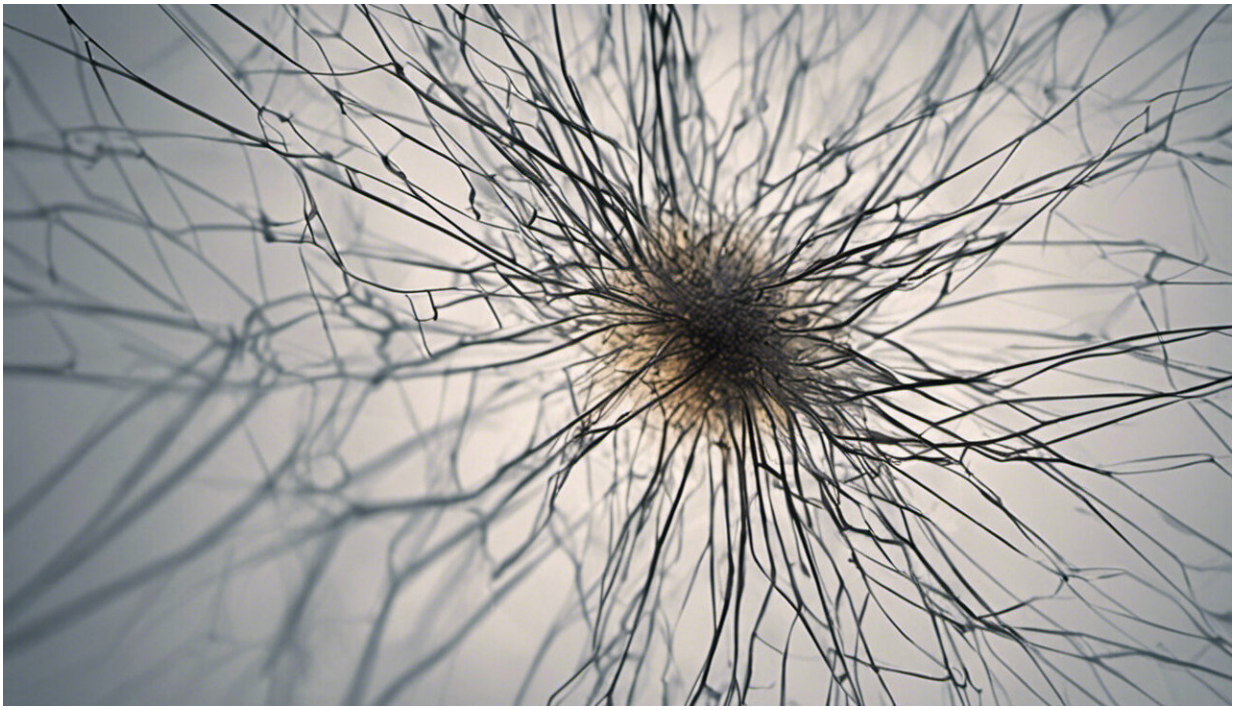
Could computer vaccines start a new approach to preventing cyber-attacks?

September 13 2017, by Paul Levy



Credit: AI-generated image (disclaimer)

There were 638m attempted ransomware cyber-attacks in 2016, according to one report. And with several high-profile attacks already committed this year, the numbers for 2017 may be even higher. Perhaps it's time then for a new approach to tackling cyber-attacks, one that focuses not on defending against them but preventing them from

happening in the first place.

Some cyber-security experts are already working on what they describe as "vaccines" to stop attacks reaching our computers or data. But this kind of prevention could just be the start. If we can avoid metaphors that imagine computers as things that need defending and instead use new words that don't suggest ways to attack them, then we might be able to develop far more effective preventative technologies.

In the case of the recent Petya ransomware attack, researchers developed a vaccine in the form of a single computer file that would instantly disable one type of virus as soon as it infected a computer, before it could cause any damage. This is different from traditional anti-virus software that tries to spot and remove any malware on a computer, but this could be after it has done its work.

This approach has been little used until now and could, at least in the short term, offer a slightly different approach to cyber-security. But vaccines are still a way of addressing viruses after they have been downloaded. Even defences such as firewalls try to stop attacks from reaching a computer but they don't prevent the attack in the first place. If we want to move to a more genuinely preventative approach, we may need to change something that fundamentally influences how we think about technology, the language we use to describe it.

From the earliest days of computers, metaphors from the physical world were used to make this new digital realm accessible and understandable to human beings like you and me. On the positive side, words such as desktop and file, folder and memo were recognisable from office life and home. On the negative side, we also transferred into cyberspace many of the very problems computers promised to solve.

And so today many "inboxes" are more cluttered than they ever were

when they held paper. Our folders are chaotically organised and we send and receive more messages and mails. There's evidence that we are no more productive today than we ever were. And there's evidence also that our virtual homes are equally vulnerable to break-in.

Ransomware attacks, such as the high-profile ones carried out earlier this year, also borrow terms from the physical world, leaving our computers "frozen" and even damaged unless we "pay up". In this case it is the realm of the highwayman as we are held to "ransom". Stick 'em up! Your money or your virtual life. Over time, these attackers become better at what they do, vying for the position of almost legendary cyber Dick Turpins.

Credit: AI-generated image (disclaimer)

The way we protect our computers follows a similar pattern. By borrowing these physical world concepts we have also replicated the risks associated with them. A firewall points to a physical wall, but even thick walls can be scaled or tunnelled under via a "worm". Our computers are akin to castles, with protective walls and guards on duty, ready for attacks from all sides. Windows PCs come with their own "Defender" software.

New language

The alternative is to create new words and images for the digital realm. These can pose different problems but also offer new opportunities. Take, for example, Blockchain technology, a system for securely recording online transactions.

There are differing views about how secure blockchain really is, but the balance of expert opinion is that it is more secure than mainstream business transacting (such as traditional online payment systems). This could be related to the fact that the word itself doesn't evoke the physical world so easily. It is harder to grasp what it is just from the word.

Another example is the word "encryption", which is viewed by many experts as a relatively secure way to prevent cyber break-ins to messages, shared data and transactions. Here security has been more successful than relying primarily on password protection (though not foolproof).

There's also Ethereum, a type of blockchain technology. At its simplest, Ethereum is a way to build decentralised applications (software programs run by a network of computers rather than being controlled by a single server). It has recently called the most secure, public blockchain.

Again, the word "ethereum" is not drawn from the mundane physical world. Its success could be related to the more elusive metaphor of

"ether" that it suggests. How do you hold ether to ransom? It suggests something more diffuse and harder to specify.

So, perhaps it's time to ditch the lazily invoked physical phrases and to get creative. Let's engage in the digital realm as a positive more alien place. It might become harder to grasp and we might have to think more carefully about it, but it might also become harder to hack too.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Could computer vaccines start a new approach to preventing cyber-attacks? (2017, September 13) retrieved 28 April 2024 from https://techxplore.com/news/2017-09-vaccines-approach-cyber-attacks.html