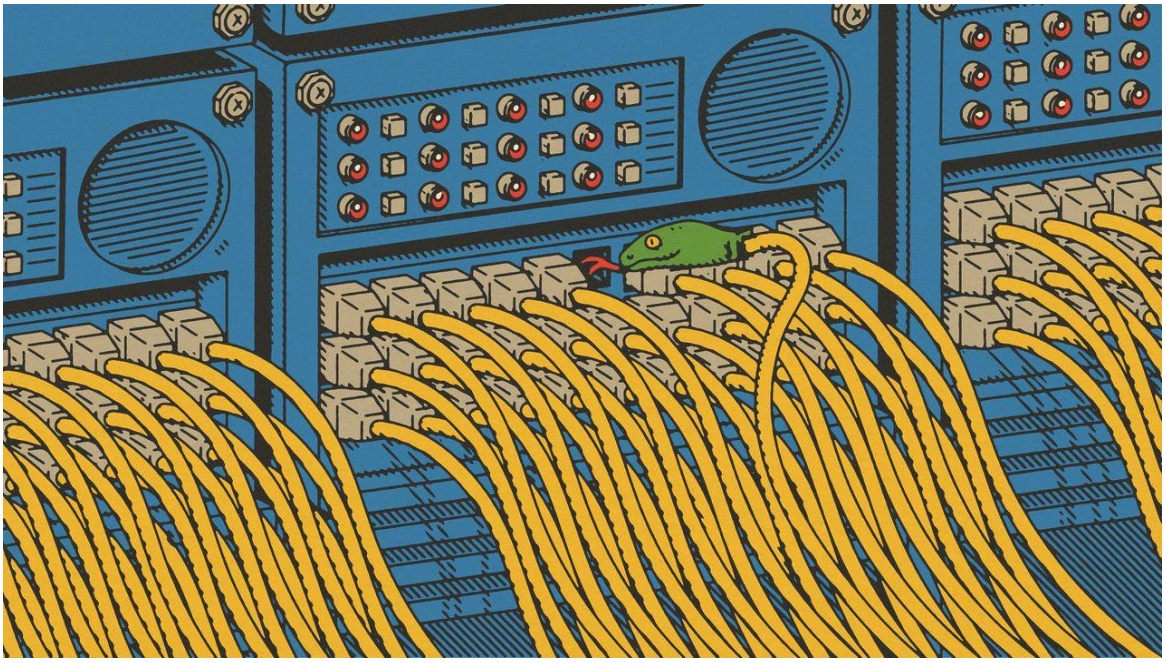
The Economist

A chilling near-miss shows how today's digital infrastructure is vulnerable

This is how to protect the internet from malicious attacks



April 4, 2024

Few inventions in history have been as important for human civilisation and as poorly understood as the internet. It developed not as a centrally planned system, but as a patchwork of devices and networks connected by makeshift interfaces. Decentralisation makes it possible to run such a complex system. But every so often comes a chilling reminder that the whole edifice is uncomfortably precarious.

On March 29th a lone security researcher announced that he had discovered, largely by chance, a secret backdoor in xz Utils. This obscure but vital piece of software is incorporated into the Linux operating systems that control the world's internet servers. Had the backdoor not been spotted in time, everything from critical national infrastructure to the website hosting your cat pictures would have been vulnerable.

The backdoor was implanted by an anonymous contributor who had won the trust of other coders by making helpful contributions for over two years. That patience and diligence bears the fingerprints of a state intelligence agency. Such large-scale "supply chain" attacks—which

target not individual devices or networks, but the underlying software and hardware that they rely on—are becoming more frequent. In 2019-20 the svr, Russia's foreign-intelligence agency, penetrated American-government networks by compromising a network-management platform called SolarWinds Orion. More recently Chinese state hackers modified the firmware of Cisco routers to gain access to economic, commercial and military targets in America and Japan.

The internet is inherently vulnerable to schemes like the xz Utils backdoor. Like so much else that it relies on, this program is open-source—which means that its code is publicly available; rather like Wikipedia, changes to it can be suggested by anyone. The people who maintain open-source code often do so in their spare time. A headline from 2014, after the uncovering of a catastrophic vulnerability in Openssl, a tool widely used for secure communication, and which had a budget of just $2,000, captured the absurdity of the situation: "The Internet Is Being Protected By Two Guys Named Steve."

It is tempting to assume that the solution lies in establishing central control, either by states or companies. In fact, history suggests that closed-source software is no more secure than is the open-source type. Only this week America's Cyber Safety Review Board, a federal body, rebuked Microsoft for woeful security standards that allowed Russia to steal a signing key—"the cryptographic equivalent of crown jewels for any cloud service provider". This gave it sweeping access to data. By comparison, open-source software holds many advantages because it allows for collective scrutiny and accountability.

The way forward therefore is to make the most of open-source, while easing the huge burden it places on a small number of unpaid, often harried individuals. Technology can help, too. Let's Encrypt, a non-profit, has made the internet safer over the past decade by using clever software to make it simple to encrypt users' connections to websites. More advanced artificial intelligence might eventually be able to spot anomalies in millions of lines of code at a stroke. Other fixes are regulatory. America's cyber strategy, published last year, makes clear that the responsibility for failures should lie not with open-source developers but "the stakeholders most capable of taking action to prevent bad outcomes".

In practice that means governments and tech giants, both of which benefit enormously from free software libraries. Both should expand funding for and co-operation with non-profit

institutions, like the Open Source Initiative and the Linux Foundation, which support the open-source ecosystem. The New Responsibility Foundation, a German think-tank, suggests that governments might, for example, allow employees to contribute to open-source software in their spare time and ease laws that criminalise “white hat” or ethical hacking.

They should act quickly. The xz Utils backdoor is thought to be the first publicly discovered supply-chain attack against a crucial piece of open-source software. But that does not mean it was the first attempt. Nor is it likely to be the last. ■