Client: Eskenzi
Source: The Daily Telegraph
Date: 08/04/2024
Page: 18
Reach: 317817
Value: 11661.7500

Our data centres were nearly seized by hackers – and nobody noticed

ANDREW ORLOWSKI

Individual volunteers play an extraordinarily key role in propping up global tech infrastructure

Imagine this plot for a movie. Somewhere in Nebraska lives a lonely, overworked and anxious man, whom we shall call Hank. Between feeding his cat, dealing with mental health issues and sorting out his mother's medical prescriptions, Hank also looks after some computer code. Hank isn't paid to do that – he's a volunteer. But mistakes happen, and an oversight by Hank leads to China taking control of the free world's IT systems, capturing our biggest cloud data centres, and paralysing the G7's economies.

Too far-fetched? Well, think again as such an attack just took place – and very nearly succeeded. A week ago, an audacious attempt to place a back door into the systems used by major cloud companies, and millions of businesses that depend on them, was discovered.

The malicious code allows an outsider to take control of these systems, and hackers very nearly pulled it off by taking advantage of an unpaid legion of lone volunteer coders, such as Hank, who is the start of a very long but critical supply chain that few ever examine.

Today, much of our enterprise and government computing is done in giant cloud data centres, and about 90pc of these use free, largely volunteer-run open-source Linux systems. The code is open, allowing anyone to inspect and submit code.

This is the utopian model mimicked by Wikipedia. But it means a great deal of the coding effort remains voluntary and in the hands of individual code "maintainers" such as Hank.

Over two years, attackers carefully took control of one of the crucial nuts and bolts of a Linux system: a compression library that zips and unzips files, and is used thousands of times a day in data centres.

XZ Utils was developed by Lasse Collin in 2005, and he has looked after it ever since. In 2021, Collin began to receive contributions over the internet from someone calling himself Jia Tan.

At first, these seemed like helpful and innocuous bug fixes – but all this later changed as the mysterious Mr Tan began to take increasing control.

Then on March 28, a Microsoft developer called Andres Freund found something astonishing. The tiny library that Collin maintained now contained a secret back door that stemmed from the code patches that Mr Tan had submitted – crucially allowing an attacker to take full control of the entire

Client: Eskenzi
Source: The Daily Telegraph
Date: 08/04/2024
Page: 18
Reach: 317817
Value: 11661.7500

system without anyone realising. The back door had already been distributed globally, and in the coming weeks and months would have reached many data centres too, becoming a part of our critical infrastructure.

"I'm surprised it's taken this long for this kind of attack to be mounted," says Tim Mackey, head of software supply chain risk strategy at the silicon design company Synopsys. "This may turn out to be a template for a new kind of social engineering."

These gambits are called supply chain attacks. The SolarWinds hack in 2020, which injected backdoor malware into at least 18,000 customers, including the US government, was another. Its discovery prompted Joe Biden, the president, to issue an executive order. But unlike SolarWinds, this one was carefully designed to target the social and perhaps even personal vulnerabilities of the open-source volunteers. "Keep in mind this was an unpaid hobby project," said Collin on a mailing list. It seems extraordinary that our economies rely so much on contributions from individual volunteers. How can so much economic value balance so precariously on something so fragile?

Google and Amazon are among the world's biggest companies, and the cloud computing market was worth almost half a trillion dollars in 2023, but critical parts still rely on unpaid volunteers. Almost a quarter of open source projects had just one developer accounting for more than 80pc of the code, a Harvard Business School study for the Linux Foundation found in 2023. Most had fewer than 10.

"These findings are counter to the typically held belief that thousands or millions of developers are responsible for developing and maintaining [open source] projects," the researchers wrote. Malware and spyware are constantly being uploaded to these code libraries, says Feross Aboukhadijeh, founder of security start-up Socket. Code checkers had failed to pick up the XZ backdoor, as it was so well disguised.

Around 10 years ago, vital encryption code used in every e-commerce transaction was compromised. The unfunded OpenSSL project that was responsible only got about $2,000 in donations each year. However, a subsequent increase in funding allowed it to take on paid staff.

Despite this, Synopsys' Mackey explains that code maintenance isn't considered sexy therefore it's difficult to get a bright graduate interested.

All of this poses a unique challenge for governments, many of which are busily trying to remove malevolent influence from their telecoms networks. Open source is a vital part of our infrastructure.

But it's also a high-trust model in an increasingly low-trust world. Perhaps we should start looking at how the sausage is made.