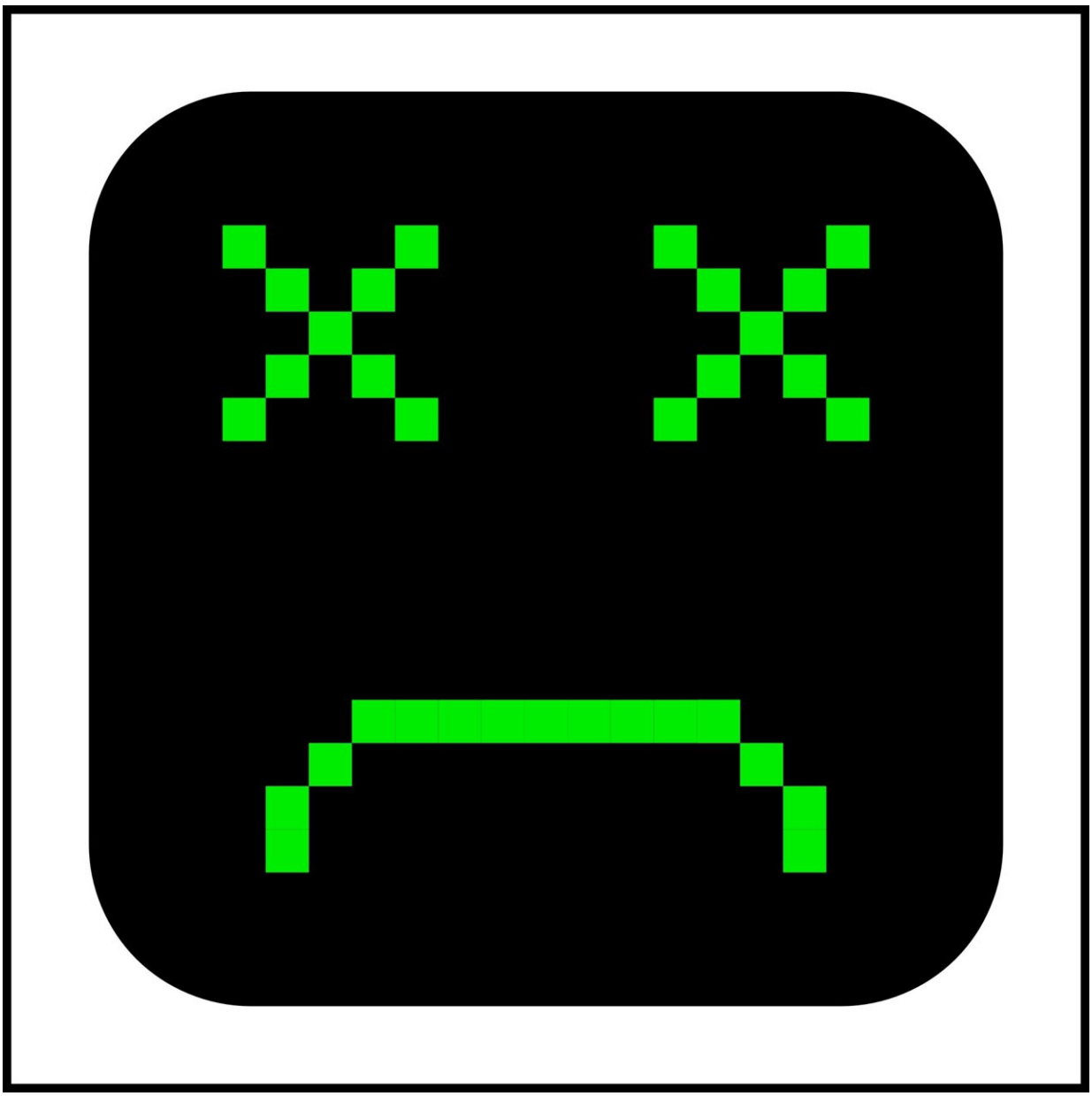
CrowdStrike crash showed us how invasive cyber security software is. Is there a better way?

July 23 2024, by Toby Murray



Credit: Pixabay/CC0 Public Domain

On Friday, the world suffered what many have described as the largest IT outage in history, when 8.5 million Windows computers crashed and wouldn't restart.

The cause was a bug triggered by an automatic update for a piece of software that until Friday nobody beyond cyber security nerds had heard of: CrowdStrike's Falcon.

Falcon is a type of software known as "endpoint detection and response," or EDR for short. It's somewhat like an anti-virus on steroids. When installed, Falcon monitors a computer for signs of cyber attacks.

It can collect data about what files you open, what programs you run, what websites you visit, and so on. This makes it highly privileged software. When an employee accidentally opens a malicious email attachment, Falcon is watching—eternally vigilant.

EDR programs are considered best practice, recommended by the Australian government's chief cyber defense agency.

Which means that in 2024, the best strategy that cyber security experts recommend involves software that spies on everything that happens on our computers.

How did we get here, and is there a better way forward?

The case for EDR

CrowdStrike is a market leader in EDR, hence why so many systems went down late last week. And there are good reasons for recommending EDR technologies like Falcon. For individual organizations, they are invaluable for alerting IT security teams to signs of cyber intrusion.

This helps IT teams to thwart an attacker before they can cause significant damage. In the case of more stealthy attacks, it helps flag suspicious behavior that could point to a long-standing intrusion. The Medibank hack of 2022 is a good example. After initially gaining access, the hacker spent weeks inside Medibank's networks undetected.

Technologies like CrowdStrike's Falcon also provide valuable intelligence about emerging cyber threats globally. Because its software is deployed in so many organizations around the world, CrowdStrike has a bird's eye view that—at least in theory—allows it to identify patterns of malicious behavior beyond what any individual organization can see.

For this reason, it's also a leader in cyber threat intelligence, providing information to IT teams about what to look out for. If an organization detects a cyber attack, data collected by EDR tools like Falcon can also help figure out exactly how the intrusion occurred.

Again, the Medibank hack serves as a good example. Federal Court filings contain detailed information about the timeline of events that led to the hack, including how the initial intrusion occurred and what the attacker did once they gained access to Medibank's networks.

Without the omniscient view provided by surveillance tools like EDR, assembling this kind of information would be incredibly challenging.

What are the downsides?

In the wake of Friday's outage, it's worth questioning the downsides of EDR technologies. Many have already raised the obvious questions about our society's dependence on too few global tech giants, and the risks of tech monocultures.

But we've known of these risks for over two decades. We likely can't expect this incident to undo the monopolies that pervade technology markets.

Another downside is the sheer technical risk. EDR software like Falcon gains its omniscience by being tightly integrated into the core of Microsoft Windows: the fundamental software that controls most of our computers. This is why it could cause the crashes we saw in the first place.

As a maker of highly privileged software, CrowdStrike had a responsibility to ensure its updates were safe. It demonstrably failed and we should all demand much higher standards of accountability from the makers of critical software.

Privacy tradeoffs

All of these issues have been widely canvassed in the days following the incident. Less discussed have been the privacy tradeoffs.

If you ask a cyber security professional to name what type of software spies on everything you do on your computer, chances are they'll name spyware before mentioning EDR.

Spyware is malicious software hackers install on victims' computers to capture sensitive information, such as passwords, banking information, or nude photos, among other things.

Indeed, some privacy-conscious computer scientists equate EDR with spyware.

As with other forms of corporate surveillance, there is a clear tension between the individual right to privacy and the organizational imperative to protect itself from cyber intrusions.

EDR technologies have been rolled out across major organizations with little debate about their impact on user privacy and trust. This outage may provide an opportunity to finally have those debates.

Is there a better way?

In the wake of this incident it's worth considering whether the tradeoffs made by current EDR technology are the right ones.

Abandoning EDR would be a gift to cyber criminals. But cyber security technology can—and should—be done much better.

From a technical standpoint, Microsoft and CrowdStrike should work together to ensure tools like Falcon operate at arm's length from the core of Microsoft Windows. That would greatly reduce the risk posed by future faulty updates. Some mechanisms already exist that may allow this. Competing technology to CrowdStrike's Falcon already works this way.

To protect user privacy, EDR solutions should adopt privacy-preserving methods for data collection and analysis. Apple has shown how data can be collected at scale from iPhones without invading user privacy. To apply such methods to EDR, though, we'll likely need new research.

More fundamentally, this incident raises questions about why society continues to rely on computer software that is so demonstrably

unreliable. Especially in Australia where we are internationally recognizedworld leaders in engineering highly secure computer systems, such as those that protect highly classified information.

In the long term, we should reduce our dependence on invasive technologies like EDR by focusing our efforts on building software that's reliable and secure in the first place.

Provided by The Conversation