

Major Information Technology (IT) outage brings businesses around the world to a standstill - expert explains what happened and why

Saturday 20 July 2024, by [The Conversation](#), [WOODWARD Alan](#) (Date first published: 19 July 2024).

The problem was traced to a single Microsoft Windows update related to the firm CrowdStrike, but it could take days for companies to recover.

A major IT [Information Technology] outage has hit businesses across the world, grounding planes as well as affecting banks and the healthcare sector.

George Kurtz, CEO of IT security firm CrowdStrike, said it had traced the issue to a “[defect found in a single content update](#)” for the security software it provides for the Microsoft Windows operating system on computers.

Microsoft said the issue was caused by an “update from a [third-party software platform](#)” and that the “[underlying cause](#)” had now been fixed.

The Conversation spoke to Professor Alan Woodward, an expert in cybersecurity at the University of Surrey, about what went wrong and how the problem could be resolved.

The Conversation - Can you explain what's happened here?

Professor Alan Woodward - I think there are two things. First, Microsoft seems to have had a problem with its Azure cloud computing platform. It's a bit unclear, but there was a degree of degradation in that service starting in the evening of 18 July. However, it didn't fail altogether.

But by far the bigger problem seems to be an update that appears to have been done in the late evening of July 18 for [IT security company] CrowdStrike's Falcon product - a computer threat checker. Falcon works by having some “agent” software deeply embedded in the operating system of every PC running Windows, which monitors that computer and “calls home” if there's a problem. It also receives updates on what to look out for if there's a threat. It's used a lot by large organisations throughout the world, which have a huge number of PCs to police.

I'm sure CrowdStrike are urgently investigating what happened. This piece of software is designed to protect people from [ransomware attacks](#) and the like. From the latest information I've seen, it looks like the update system file was somehow released in an incorrect format.

The Windows operating system gets to this update and it doesn't know how to cope, so it crashes. That's why people have been getting the “blue screen of death” [a computer screen with an error message indicating a system crash].

And the big problem is, you can't fix this issue remotely. You have to go into every machine separately and put it into "safe" or "recovery" mode to isolate the software. From there, you should be able to reboot the machine and get it up and running again. But if you're a big global company with a large distributed IT estate, that's going to take a long time.

Why has this outage had such wide-ranging effects?

CrowdStrike has been a great success - its security software is used by hundreds of thousands of major clients around the world. So airlines, airports, railways, hospitals, stock exchanges ... they're all going down.

It started in Australia when they got up for business on Friday. The update had clearly been sent out last night UK time, and it has just rippled around the world.

With deliberate ransomware attacks, they'll typically take out one or two targets at a time. But in this case, it's happened to thousands of organisations at once. We've not had anything like this before.

How CrowdStrike will fix the software is yet to be determined. As I've explained, it's clear how companies can work around the issue. But for some very large organisations, this could affect their critical infrastructure and business for a long time yet - it's going to take them days to physically work round all those machines.

The problem also affected the healthcare sector. Ground Picture / Shutterstock

Can security companies ensure this doesn't happen again?

Security software is very intertwined with a computer's operating system - it's buried deep in there. There has to be a way that if something is found to be corrupted, it doesn't just keep crashing the system - this may have to be done in cooperation with Microsoft, which owns the Windows operating system.

There's got to be some way of backing out of it, and there is. However, most people trying to log into their blank PCs don't know how to put their PCs into safe mode and revert to a previous state.

At the moment, it looks like it's one corrupted file that's producing a global problem. Computers download updates all the time, so how Microsoft prevents that from happening with this update, I don't know. It's not immediately obvious. And the million dollar question is: how did this corrupted file get released in the first place?

How long before this problem is fully resolved?

It's certainly going to take days, if not weeks. It's like those hospitals in London that [got attacked with ransomware](#). They're still suffering - there's a very long tail on these things.

And in this case, it's not just a long tail but a very broad swathe of global organisations in transport, health and everywhere else. I don't think we've seen anything like this before.

On X, formerly Twitter, George Kurtz, co-founder and CEO of CrowdStrike, [commented](#): "The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates."

[Alan Woodward](#), Professor, Department of Computer Science, [University of Surrey](#)

P.S.

- The Conversation. Publié: 19 juillet 2024, 14:25 CEST Mis à jour le : 19 juillet 2024, 19:51 CEST.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

- [Alan Woodward](#), [University of Surrey](#)

Alan began as a physicist. However, he developed an interest in computing early on through signal processing for gamma ray burst detectors, and so switched to engineering after his BSc. His post graduate research at the Institute of Sound and Vibration Research (ISVR), University of Southampton, was in adaptive filtering, and novel methods of recovering corrupted signals. Alan also worked on novel methods of noise cancellation, both passive and active.

After leaving the ISVR Alan worked for the UK government for many years and subsequently provided advice for some years. He has particular expertise in, and continues to conduct research into, cyber security, covert communications, forensic computing and image/signal processing. Alan has been involved in some of the most significant advances in computer technology which have seen him elected as a Fellow and chartered member of the British Computer Society, Institute of Physics and the Royal Statistical Society.

In addition to his academic and government work, Alan has run businesses focussed on various aspects of Information Technology (IT). In 2000 Alan was pivotal in the flotation of Charteris plc on the London Stock Exchange. He remained a director until 2008 at which point he began to focus back on his academic interests. Alan continues to be a director on businesses involved in IT.

Although Alan has been at the leading edge of technology development for many years, he is primarily a particularly good communicator. He is known for his ability to communicate complex ideas in a simple, yet passionate manner. He not only publishes in the academic and trade journals but has articles in the national press and comments on TV and radio. Despite the length of his experience, his hands-on ability with emerging technologies contributes significantly to the respect he is repeatedly shown when he leads teams where technology is involved.

- The Conversation is a nonprofit news organization dedicated to helping academic experts share ideas with the public. We can give away our articles thanks to the help of foundations, universities and readers like you. [Donate Now to support research-based journalism](#)