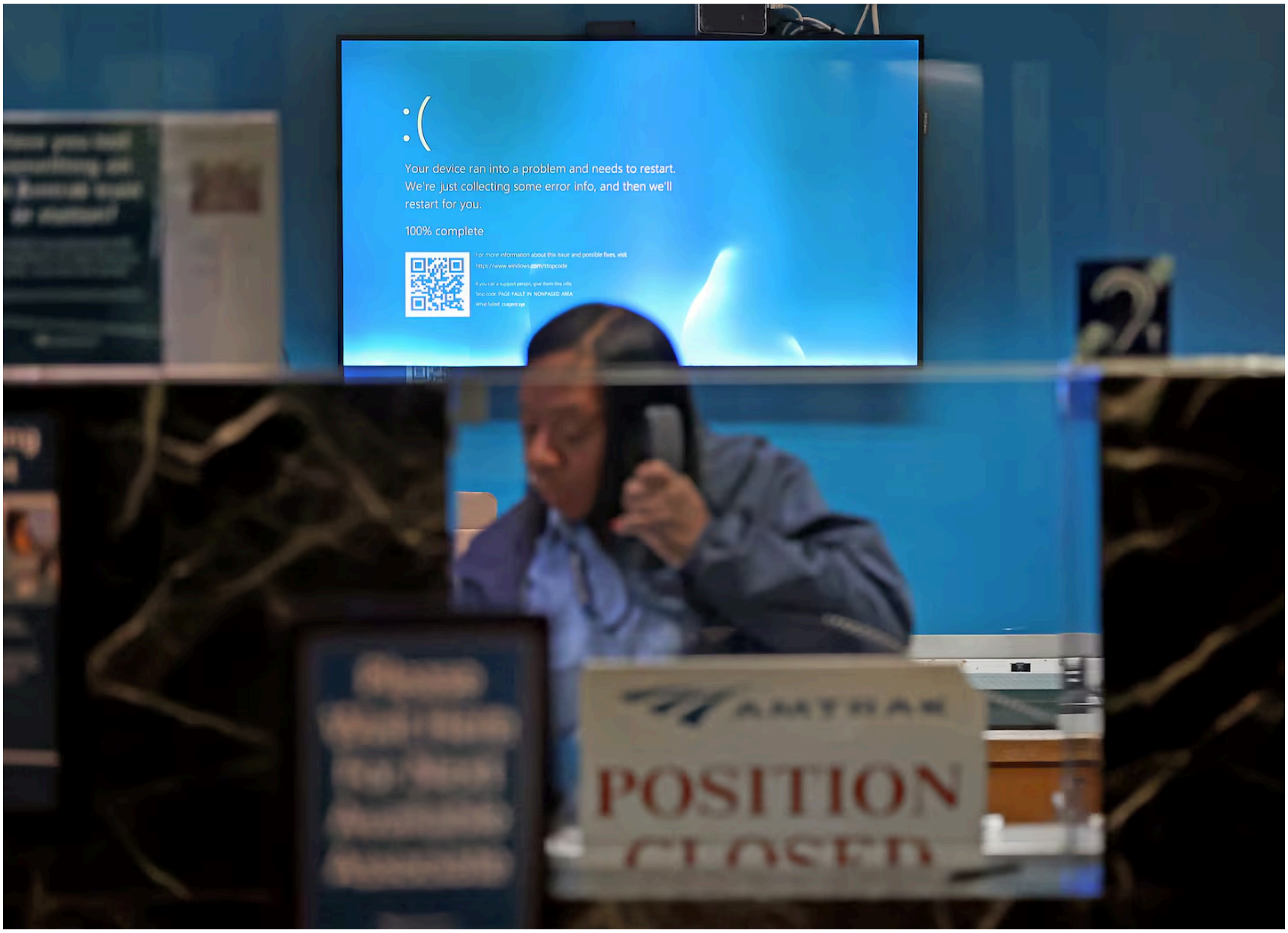
TECH LAB

How errant keystrokes at CrowdStrike led to a global outage of Microsoft networks

By Hiawatha Bray Globe Staff, Updated July 19, 2024, 12:39 p.m.


:(
Your device ran into a problem and needs to restart.
We're just collecting some error info, and then we'll restart for you.
100% complete
AMTRAK
POSITION
CLOSED

A "blue screen of death" was displayed at the AMTRAK ticket desk at South Station Friday morning. DAVID L. RYAN/GLOBE STAFF

It took just a few errant keystrokes by someone at the Texas cybersecurity firm CrowdStrike to cause a digital meltdown that has afflicted millions of computers around the world.

Understanding what happened requires a crash course in cybersecurity.

Our home computers rely on security software that runs on individual machines and is regularly updated to detect the latest threats. But that’s not good enough for businesses and government agencies. They’re under relentless attack by professional criminals and foreign intelligence services that keep finding new ways to break in and steal data.

CrowdStrike fights back with an artificial intelligence system called Falcon, which monitors its customers’ computers around the clock, according to information from the company’s website and regulatory filings. By training the AI on the data that flow in and out of these devices, Falcon can quickly recognize new attacks and shut them down before they do too much damage.

CrowdStrike’s technology is used in more than 29,000 enterprises worldwide, including companies such as Intel, Target, and Salesforce; state agencies in Oklahoma and Illinois; and cities such as Phoenix and Las Vegas.

The system requires installing Falcon software on every digital device on the network — desktop computers, laptops, servers, even smartphones. On Thursday night, CrowdStrike issued an update to this software for computers running Microsoft’s Windows operating system. For reasons yet unknown, the update contained a bug so severe that once it was installed, the Windows computer could no longer boot up properly and began displaying the notorious “blue screen of death.”

Happily, the bad code wasn’t fed to devices running non-Windows operating systems, including computers that use the Linux or Apple Mac operating systems. Smartphones weren’t affected, either. But Windows machines dominate in business and government offices. And millions of them crashed, creating a global fiasco.

And now comes the hard part, according to Craig Shue, head of the computer science department at Worcester Polytechnic Institute. The affected computers will have to be repaired by knowledgeable technicians, who will have to boot the computers in "safe mode," then delete and replace the defective Falcon software. Rinse and repeat for every PC on the premises.

"That's what's going to slow down the recovery on this," said Shue. "If you've got a thousand computers, that's going to take somebody a while to do."

It's tempting to blame Microsoft for this. Shouldn't the company have designed Windows so it couldn't be ravaged by a mere software update? Not in this case, said Shue, because cybersecurity software is so different from ordinary software apps.

Most apps can't access the basic functions of the computer. Instead, they rely on the operating system. So when you print a document using Microsoft Word, the software asks the operating system to forward the file to the printer. This way, a bug in Word would only affect Word; the rest of the machine is unaffected.

Shue said that unlike other apps, cybersecurity programs like Falcon are almost as powerful as the operating system. They must be, to prevent the computer from running toxic software or carrying out illicit commands. And when something goes wrong — as we've seen — a bug in a cybersecurity program can debilitate the computer or make it totally inoperable.

"It can basically do anything on the computer," said Shue. "It can delete any file. It can stop any program from running. And that's really important when you're fighting a virus."

If Microsoft denied this level of access to outside cybersecurity vendors, the company could face an antitrust lawsuit for seeking to force companies to use only Microsoft's own cybersecurity services, Shue added.

Microsoft did not immediately respond to a request for comment.

Stuart Madnick, professor of information technology at the MIT Sloan School of Management, expects the hits to keep on coming because so many companies depend on certain IT vendors, such as CrowdStrike.

As a result, a bug in the vendors' software, whether accidental or deliberate, can affect companies all over the world. That's why cybercriminals try to hack the software sold by these vendors, as a way to gain illicit access to dozens or hundreds of organizations at a single stroke.

"This is happening more and more often," said Madnick, "and the consequences are larger and larger."

He cited the 2020 incident when hackers compromised software from SolarWinds, a maker of network management tools used by companies worldwide. The hackers stole data from a host of major organizations, including the US departments of State, Homeland Security, Commerce, and Treasury.

Another example: last year's compromise of MOVEit, a file transfer program made by Burlington-based Progress Software. Hundreds of enterprises worldwide were affected by that attack, which enabled criminals to download sensitive files.

Madnick warned that even worse breakdowns could happen. For instance, most personal computers and servers use software on a built-in chip to boot up the system. A defective update to this software, issued mistakenly or on purpose, could render millions of personal computers unbootable.

"Basically, it can turn your laptop into a brick," Madnick said. "You take your laptop, drop it off at the local dump, and buy a new one."

Multiply by millions of machines, and uh-oh.

Hiawatha Bray can be reached at hiawatha.bray@globe.com. Follow him @GlobeTechLab.

💬 Show 87 comments