# Boeing hit by WannaCry virus, but says attack caused little damage

Originally published March 28, 2018 at 3:16 pm *Updated March 28, 2018 at 9:16 pm*

Workers assemble aircraft at Boeing's plant in North Charleston, S.C., where the cyberattack started. (Bruce Smith/AP)

**Though news of the attack by the WannaCry virus triggered widespread alarm within Boeing and among airline customers during the day Wednesday, by evening the company was calling for calm.**

By Dominic Gates

*Seattle Times aerospace reporter*

Boeing was hit Wednesday by the WannaCry computer virus, and after an initial scare within the company that vital airplane-production equipment might be brought down, company executives later offered assurances that the attack had been quashed with minimal damage.

Though news of the attack triggered widespread alarm within the company and among airline customers during the day, by evening Boeing was calling for calm.

“We’ve done a final assessment,” said Linda Mills, the head of communications for Boeing Commercial Airplanes. “The vulnerability was limited to a few machines. We deployed software patches. There was no interruption to the 777 jet program or any of our programs.”


**Related stories**

How to protect yourself from ransomware attacks

Atlanta hobbled by major cyberattack that mayor calls ‘a hostage situation’

Wire-transfer scheme, ransomware attack — tiny Yarrow Point finds itself in criminals’ crosshairs

Baltimore: Ransomware attack hobbled city’s dispatch system


Earlier in the day, when the cyberattack struck, the reaction was anything but calm.

Mike VanderWel, chief engineer at Boeing Commercial Airplane production engineering, sent out an alarming alert about the virus calling for “All hands on deck.”

“It is metastasizing rapidly out of North Charleston and I just heard 777 (automated spar assembly tools) may have gone down,” VanderWel wrote, adding his concern that the virus could hit equipment used in functional tests of airplanes ready to roll out and potentially “spread to airplane software.”

VanderWel’s message said the attack required “a batterylike response,” a reference to the 787 in-flight battery fires in 2013 that grounded the world’s fleet of Dreamliners and led to an extraordinary three-month-long engineering effort to find a fix.

“We are on a call with just about every VP in Boeing,” VanderWel’s memo said.

It took until late Wednesday afternoon before Boeing issued a statement dialing back the fears.

“It took some time for us to go to our South Carolina operations, bring in our entire IT team and make sure we had the facts,” Mills said.

Even then, the afternoon statement was short on detail.

“Our cybersecurity operations center detected a limited intrusion of malware that affected a small number of systems,” it said. “Remediations were applied and this is not a production and delivery issue.”

Speaking Wednesday evening, Mills said the speculation in VanderWel’s message that some 777 production equipment might have gone down turned out not to be true.

She added that the attack was limited to computers in the Commercial Airplanes division and that the military and services units were not affected.

“To the best of our knowledge,” she said, the crisis is over and the attack did no significant damage.

## How did it happen?

The WannaCry virus, which exploits a flaw in Windows software to gain access to a network, attacks computers using “ransomware.”

It was designed to lock users out of their data by encrypting files until they pay a fee, sometimes in cryptocurrency, or other type of ransom.

Ransomware attacks have increased in recent years. The city of Atlanta experienced a five-day ransomware attack that was mostly fixed by Tuesday.

However, Jake Williams, founder of cybersecurity consultancy Rendition Infosec, said the ransomware part of the WannaCry virus is broken and there’s actually no way to pay a ransom that will retrieve files once encrypted.

The sole purpose for a hacker to deploy it is to damage computer systems.

The WannaCry virus first surfaced in a May 2017 worldwide cyberattack. Once a single computer is infected, it can spread to all Windows computers on a network.

At the time, the Trump administration blamed North Korea for the attacks.

Microsoft issued patches to plug the vulnerability. However, Corey Nachreiner, chief technology officer of Seattle security technology firm WatchGuard Technologies, said some companies with specialized equipment don’t update very often for fear their custom-built systems will be in danger.

Microsoft declined to comment on the Boeing cyberattack.

Mitchell Edwards, a Dallas, Texas-based cyberthreat intelligence analyst, said that although a so-called “kill switch” fix for the WannaCry virus was quickly developed, other hackers were also quick to produce WannaCry variants that could defeat the fix.

He said the virus used to attack Boeing could have been one of these updated WannaCry versions.

Mounir Hahad, head of Juniper Threat Labs at Juniper Networks, said the infection could potentially have come from a dormant version of the original virus.

He explained that the “kill switch” fix only works when a computer is connected to the internet. If the machine is rebooted when on a local network that’s not connected to the internet, the virus would resume the infection process.

## Production systems hit

Whatever happened Wednesday with Boeing, the WannaCry threat to manufacturing businesses is real.

Williams of Rendition Infosec said he knows of three manufacturing companies, two of them now his clients in the United States, that suffered production stoppages because of WannaCry infections in the last six months.


## More on Boeing & Aerospace

Some airport workers still earn less than minimum wage, as Sea-Tac law leaves a confusing patchwork

Flow International to move Kent manufacturing work to Kansas, lay off 110

More 737 fuselage problems cloud Boeing’s plan to ramp up production

Boeing faces slowdown in 737 fuselage deliveries from Spirit AeroSystems

Trump Russia announcement catches Boeing off guard; spying an everyday concern for defense contractor

Monday Memo: Saudi Crown Prince visit, Seattle-area home prices, Friday market holiday


He said one plant was down for 24 hours, another for 96 hours. In both cases, configuration files that controlled machines were lost and systems had to be reinstalled from scratch before production could restart.

He declined to name the companies because of nondisclosure agreements.

“Tons of manufacturing equipment runs on Windows. I was surprised,” Williams said.

In addition, he said, some factory equipment runs on Windows Embedded, which is a variant of the operating system used in computer-controlled machines.

An infection of the Windows Embedded machines “absolutely will bring down a plant,” he said.

However, cyber experts judged one “nightmare scenario” that spread on social media Wednesday to be extremely unlikely.

Once the Boeing cyberattack news broke, some on Twitter suggested the virus could perhaps infect an airplane's control software and trigger a ransomware demand while in the air.

Edwards dismissed this as "hysteria." Williams agreed.

"I don't think that's realistic," Williams said. "I don't think any of Boeing's planes or any aircraft anywhere run Embedded Windows. It's not suitable for applications that require consistent, real-time availability without delay because lives depend on it."

In contrast, Williams said the threat to production systems is real, though solvable.

"I've seen three stoppages in the last six months, and I don't think this will be the last," he said. "If you are in manufacturing today, you need to do some preparations. It's easy to shut (WannaCry) down."

His company has produced a free software fix called Tearstopper that he said prevents WannaCry viruses from encrypting files.

*Dominic Gates: 206-464-2963 or dgates@seattletimes.com*
*Seattle Times technology reporter Rachel Lerman contributed to this report*

View 50 Comments

Next Story
**Flow International to move Kent manufacturing work to Kansas, lay off 110**

Previous Story
**More 737 fuselage problems cloud Boeing's plan to ramp up production**

Contact