Dropbox and Similar Services Can Sync Malware

By David Talbot

Published: 2013-08-21 · Archived: 2026-04-06 00:23:21 UTC

Dropbox and similar services have exploded in popularity in recent years because users find it so convenient to simply drag files to an icon that puts that data in the cloud, shares it with others, and automatically syncs new versions across multiple devices.

But ease of use and insecurity often go hand in hand, and now researchers are revealing an uncomfortable truth: if a computer with Dropbox functionality is compromised, the synching feature allows any malware installed by the attacker to reach other machines and networks using the service. “People don’t consider that once you have Dropbox configured, anything you put in the synchronization folder gets a free pass through the firewall,” says Jacob Williams, a digital forensic scientist at CSR Group. “We’ve tested this on several services, and it gets data right through the firewall.”

Williams says that in recent weeks, he has been able to do this not only with Dropbox but also with competing services: SkyDrive, Google Drive, SugarSync, and Amazon Cloud Drive. “This is like e-mail in the ’90s,” he says. “We wanted it, but with it came spam, malware command and control, and malware distribution. We just don’t have detection and security tools to cover Dropbox and similar services yet.”

No one at Dropbox, which was founded in 2007 by Drew Houston and Arash Ferdowsi (see “Hiding All the Complexities of Remote File Storage Behind a Small Blue Box”), would comment on the matter. The service has more than 175 million users.

The research on Dropbox and similar services adds to a litany of recent security concerns over storing data and doing computation on remote or “cloud” servers. While such services can be better than running everything yourself (see “Being Smart about Cloud Security”), security researchers keep finding new ways to attack them (see “Security Researchers Rain on Amazon’s Cloud”). “With the increasing use of cloud-based services, these kinds of attacks are going to reappear until the platforms mature,” says Radu Sion, a computer scientist and security reasearcher at Stony Brook University. “The attack here is not in fact on Dropbox but rather in the people’s use of Dropbox. Dropbox just facilitated a channel for [infected] documents through the corporate firewall.” He called it “a well-put-together combination of existing exploits.”

Williams stumbled onto exploiting Dropbox as an attack vector when a client asked him to test the security of a corporate network. As a first step, unrelated to Dropbox, Williams obtained a personal e-mail address for the CIO and successfully carried out a “spear-phishing” attack when the CIO clicked on an attached file containing malware. When the CIO was away from the office with his laptop, Williams was able to get access to the computer—and found corporate documents in a Dropbox synchronization folder.

This by itself wasn’t Dropbox’s fault; everything on the machine—passwords, family photos—was exposed. But the crucial next step involved using Dropbox and its synching powers to load a malware file that would then appear in folders inside the corporate network.

He wrote a malicious file called DropSmack and used it to infect a file already in the CIO's Dropbox folder. When the CIO next opened that file, the DropSmack tool then allowed malicious commands to be sent inside the corporate network via files synchronized by Dropbox—including commands that allowed files to be stolen. Later, Williams replicated the attack with several other popular cloud-storage synching services.

While no attacks are known to have occurred this way, "I can't imagine someone somewhere hasn't been using it for actual attacks," Williams says. "It's nearly impossible to detect with current tools, so we don't know. Data loss prevention tools have a really hard time with Dropbox and the like. They really fail at protecting these services." He discussed his attacks on cloud storage services in a talk at Black Hat earlier this month.

In a further finding last week, other researchers were able to decrypt the code used by the Dropbox client—the precursor to an attack on Dropbox itself. "I would say it was kind of an easy task—the code was protected in a pretty much simple way," said Przemysław Węgrzyn, a software engineer at Codepainters, a security firm in Wroclaw, Poland, who co-wrote a paper delivered at the Usenix security conference in Washington, D.C. "Basically, if you can reverse-engineer it, you can see how it communicates, see everything about the communication, about what kind of security it is, and what level to attack it."

Węgrzyn himself downplayed the significance of this, however, since it was not an actual successful attack on Dropbox and resulted in no data loss.
