Code Hosting Service Shuts Down After Cyber Attack

By Brian Prince

Published: 2014-06-20 · Archived: 2026-04-05 20:15:01 UTC

A code hosting company has shut down following a cyber attack that erased much of its data, backups, machine configurations, and offsite backups.

The company states in a message on its homepage:

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of ongoing credibility.

Visitors to the Code Spaces website are greeted with a lengthy outline of what happened. On Tuesday, the company explains, Code Spaces was hit by a distributed denial-of-service attack against its servers. Such attacks weren't uncommon. Unfortunately, this time it was just the beginning.

The unknown attacker was able to gain access to Code Spaces' Amazon EC2 control panel, and left a number of messages for the company to contact them using a Hotmail address. Doing so yielded an extortion demand. When the company realized the attacker had access to the EC2 control panel, further investigation revealed the person also had access to the data in the company's systems, although no machine access occurred, because the intruder did not have the private keys.

The company statement continues:

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel. We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances.

Patrick Thomas, security consultant for Neohapsis, calls the situation a "nightmare scenario" for cloud services companies:

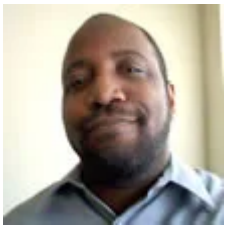
This is a wakeup call to other organizations that have critical assets on cloud services. Two-factor authentication and detailed event monitoring and alerting are essential components of any cloud strategy.

Offsite backups have been considered a necessary operating procedure for any sensitive data, but in the age of cloud infrastructure many organizations think that they can simply pass the buck on backups, getting their geographic distribution and redundancy for free as part of going to the cloud. However, anything that's vulnerable to the same threats isn't fulfilling the original intent of offsite backups. Perhaps it makes more sense to start talking in terms of diversified backups, to emphasize the broad types of threats that a backup strategy must mitigate.

Jim Reavis, chief executive officer of the Cloud Security Alliance, stresses that DDoS attacks and other malicious activity have caused business outages and shutdowns before among companies using traditional IT, and that cloud computing itself was hardly a factor in exacerbating Code Spaces' demise. He told me in an email:

Cloud users of IaaS [infrastructure-as-a-service] like Code Spaces have significant responsibilities in implementing security best practices to protect their system availability and proprietary information, as we have outlined in our security guidance and controls framework. At a high level, tenancy with a robust cloud computing infrastructure should provide greater pipes to withstand DDoS attacks than a small business could afford.

About the Author



Contributing Writer, Dark Reading

Brian Prince is a freelance writer for a number of IT security-focused publications. Prior to becoming a freelance reporter, he worked at eWEEK for five years covering not only security, but also a variety of other subjects in the tech industry. Before that, he worked as a news reporter for the Asbury Park Press, and reported on everything from environmental issues to politics. He has a B.A. in journalism from American University.
