



Tech Center: **Cloud Security**

 E-mail this page |  Print this page |  BOOKMARK 

Cloud Services Credentials Easily Stolen Via Google Code Search

Public cloud services are not safe for storing sensitive data, researchers say

Nov 09, 2011 | 07:21 PM | [2 Comments](#)

By **Tim Wilson**
Dark Reading

The access codes and secret keys of thousands of public cloud services users can be easily found with a simple Google code search, a team of security researchers says.

Researchers at Stach & Liu, a security consulting firm that develops Google hacking tools, first [revealed the results of their cloud services research](#) (PDF) at the Hacker Halted conference last month in Miami. Now the team is offering one word of advice to companies that are considering storing critical information on the public cloud: Don't.

"It is not a good idea to put sensitive data out in the cloud right now -- at least not until there are intrusion-detection systems that would let users see these types of searches on their cloud services," says Fran Brown, managing director at Stach & Liu. "Companies are pushing forward on the cloud because they want the functionality, but they're not seeing the risk."

In an online demonstration, Brown showed how an attacker who knows Google and some simple facts about cloud services authentication can easily find the access codes, passwords, and secret keys needed to unlock data stored in public cloud services environments such as Amazon's EC3.

Such data is routinely stored by application developers and system administrators who don't know that their simple text files might be indexed by search engines and discoverable with a simple Google code search, Brown says.

"We found literally thousands of keys stored this way, any one of which could be used to take control of computers in the cloud, shut them down, or used to launch attacks on other computers on the same service," he states.

The problem, according to Stach & Liu, is not necessarily the service provider, but the developers and administrators who store their credentials carelessly in text files and applications code that might be exposed to the Web, particularly in Web-based cloud environments. "All you need is one

Cloud Security Reports



Dark Side of the Cloud Becoming Clearer

Recent high-profile breaches against cloud-based services have forced tougher security and closer scrutiny of what to put in the cloud.



Spot Trouble in the Cloud: Adapting Security Monitoring & Incident Response

Security monitoring, incident response and forensics are essential, even in the cloud. But the cloud by definition implies relinquishing at least some control, which can make these practices problematic. In this report, we identify the challenges of detecting and responding to security issues in the cloud and discuss the most effective ways to address them.



Cloud Security: Understand the Risks Before You Make the Move

Security concerns give many companies pause as they consider migrating portions of their IT operations to cloud-based services. But you can stay safe in the cloud. In this Dark Reading Tech Center report, we explain the risks and guide you in setting appropriate cloud security policies, processes and controls. Plus: How to catch up when security is an afterthought to a cloud migration.



Cloud Security Newsfeed

[PerspecSys Launches Enterprise-Grade Cloud Security Solution](#)

[RSA Announces More Secure User Access To Microsoft Cloud Services And Applications](#)

careless developer who puts his credentials in a text file -- and you're hosed," Brown says.

Stach & Liu has developed a cloud-hacking tool -- another in its [Diggy line of Google hacking tools, which were first unveiled at Black Hat USA in July](#) -- that seeks out and finds exposed cloud credentials via a simple Google code search.

While cloud services authentication might require multiple pieces of information in order to gain access to stored data, Stach & Liu was frequently able to find all of the credentials required to access corporate data stored on the cloud, Brown says.

In many cases, cloud services agreements state specifically that the provider is not responsible for such credentials leaks, Brown observes. "If you look closely at the agreements, you'll see that the provider makes no guarantee that the data stored in the service will stay safe," he notes. "The security industry needs to broker a better deal with the Amazons and the other cloud service providers out there."

In its Hacker Halted presentation, Stach & Liu also presented several other Google hacking tools and vulnerabilities, including tools that identify malware as well as flaws in Flash and data leak prevention applications.

"Flash files are another easy attack," Brown says. "It's very easy to find login pages built on Flash, decompile the files, and look for vulnerabilities." In the demonstration, Brown was able to use Google search results to gain access to a Web-based account in less than 30 seconds.

Have a comment on this story? Please click "Comment" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

- [RackSpace And StillSecure Partner To Offer Cloud Security](#)
- [CommTouch Reports 27 Percent Increase In Revenue In Third Quarter 2011 Results](#)
- [Web Malware Up 89%. Avalanche Cybergang Re-emerges](#)
- [CloudPassage Launches Halo GhostPorts Features](#)

[MORE NEWSFEED >>>](#)

- | | |
|-----------------------------------|--|
| Advanced Threats | Insider Threat |
| Authentication | Security Monitoring |
| Cloud Security | Security Services |
| Compliance | SMB Security |
| Database Security | Vulnerability Management |

Comments

2 Comments

[Quick View](#) [Full View](#)

-- MOST RECENT COMMENT --

Encryption before the cloud

Comment by AMONTVILLE000 Nov 10, 2011, 07:58 AM EST
It seems that we really need a method of encrypting information before the cloud, and we should try to figure out a way where users needn't really worry about it. By "we" I'm pretty much referring to the cloud providers.

It seems to me that they should be working to figure this problem out.

- [Reply To Comment](#)
- [Permalink](#)
- [Share](#)
- [Email](#)
- [Report](#)

thanks for information
Comment by UnlockPDF Nov 10, 2011, 04:48 AM EST

Encryption before the cloud
Comment by AMONTVILLE000 Nov 10, 2011, 07:58 AM EST

Care to Comment?

Subject (max length: 75):

Comment: