Amazon EC2 cloud service hit by botnet, outage

Amazon's EC2 cloud service has had to deal with a botnet released through its service and a data center power failure in the same week.

Lance Whitney
Dec. 14, 2009 7:50 a.m. PT

The folks who run Amazon's EC2 cloud service must be happy the week is nearly over.

The cloud-based EC2 (Elastic Compute Cloud) was kept jumping this past week by two incidents: a compromised internal service that triggered a botnet, and a data center power failure in Virginia.

On Wednesday, security researchers for CA found that a variant of the infamous password-stealing Zeus banking Trojan had infected client computers after hackers were able to compromise a site on EC2 and use it as their own C&C (command and control) operation.

Don DeBolt, Director of Threat Research for CA Internet Security Business Unit, told CNET that the botnet first came to light while his firm was reviewing spam and found one with a URL for a piece of malware called xmas2.exe, described in a blog. After examining the file, DeBolt discovered it was a variant of the Zeus bot that was calling home to a computer inside Amazon Web Services, which houses EC2.

As a keylogger, Zeus is known to specifically capture bank account information, noted DeBolt, and was trying to perform the same crime in this case. The bot was also attempting to report the IP addresses of any clients that were infected via spam. The cybercrooks reportedly snuck their way into EC2 by gaining access through a site hosted on Amazon's service.

Once the bot was discovered, DeBolt and his team contacted Amazon to provide all the information from their client-based analysis. Since then, the files that were serving up the botnet on Amazon's side are no longer active.

Responding to a request for comment, an Amazon representative said Friday: "We take all claims of misuse of the services very seriously and investigate each one. When we find misuse, we take action quickly and shut it down...which we did in this case. Our terms of usage are clear and we continually monitor and work to make sure the services aren't used for illegal activity. We also take the privacy of our customers very seriously, and don't inspect their instances. This is part of the reason why legitimate customers of all types are comfortable running production applications on Amazon EC2."

The representative also added: "It's also important for developers who leverage cloud services to use the same security best practices that they would if they were operating in their own data center or a collocation facility. We provide security best practices to help customers protect themselves from malicious users inside or outside of the cloud."

On Saturday, Amazon also comments in more detail about the botnet through a security bulletin.

DeBolt said the botnet doesn't necessarily point to any specific flaw in Amazon's service because it's as yet unknown, at least to him, how the hackers injected the C&C files onto an Amazon server. A hole in a particular application may have opened the door, or other instances of Zeus could have captured log-in credentials, which were then used to access the necessary services hosted on EC2.

DeBolt believes this incident does raise a note of caution about using cloud-based services, but also feels that these types of increasingly common attacks are the nature of the Internet beast.

Internet beast.

"This is the first instance that we're aware of that EC2 has been compromised to be used to distribute malware," he said. "So it certainly should raise awareness. Anytime that you use a cloud-based service or a host infrastructure or applications, that increases the complexity of what you're trying to do. And if the access and application controls are not maintained securely, then it opens it up to potential compromise."

But DeBolt also said he feels this was a target of opportunity and not a target of choice against Amazon. "The service could have been on Amazon, or it could have been in somebody's basement," he added. "The malware actors don't care. They're just looking for Internet-accessible, anonymous command and control locations that they can access from anywhere around the world."

How can providers like Amazon better protect themselves? DeBolt urges them to ensure that all access controls and applications are locked down as tightly as possible to protect themselves against common Web-based vulnerabilities like cross-site scripting attacks and SQL injections.

As if a botnet attack weren't enough to deal with, also on Wednesday, one of Amazon's data centers suffered a power outage, interrupting service for several hours. Amazon's Service Health Dashboard reported connectivity and power issues for an EC2 facility in Northern Virginia. The outage itself lasted than an hour, though staff members were kept busy for several hours trying to restore and recover several customer sites, or instances.

On Thursday, the Dashboard reported that both the primary and a backup component of a redundant power supply had failed, cutting juice to a portion of the facility's servers. As a result, customers were unable to connect to their instances. Once the defective components were bypassed, servers restarted and customer instances gradually came back online.

Launched in 2006, EC2 was designed to give software developers virtual server space and resources for testing Web-based applications. Since then the service's offerings have grown to include Windows, SQL Server, and other platforms in addition to Linux, under which developers can run their apps. Amazon EC2 counts IBM among its key customers.

But EC2 has seen its share of growing pains over the years, with random though mostly short-term outages plaguing the service and angering customers. At least one other site hosted on EC2 has also been the victim of cyberattacks. In October, hosting service Bitbucket was knocked offline for a long stretch of time by a distributed denial of service (DDoS), an incident described in detail by The Register.

Updated at 2:25 p.m. PST *with a response from Amazon.*

Updated at 7:45 a.m. PST *with further response from Amazon and clarification on Don DeBolt's title.*

COMMENTS

Software | Internet | Security