

ACCESS ^{'23}

The Cloud Identity, Access, and Permissions Summit



Live Hack – Anatomy of an Identity Breach

Jeff Moncrief, Field CTO
Sonrai Security





**“Hackers Don’t Hack
Anymore...They Just Login.”**

“Identity is the New Network”

**“What Do You Do When Statistics
Prove they Just Walk Right Through
the Front Door?”**

- *Jeff Moncrief, Field CTO, Sonrai Security*

When Statistics are Actual Reality

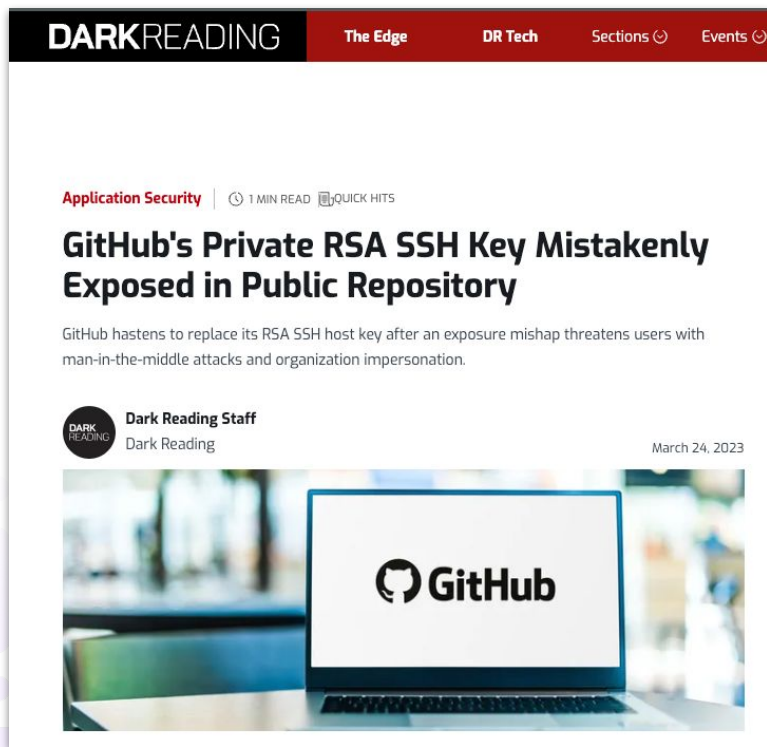
The screenshot shows the GitHub repository page for 'ramimac/aws-customer-security-incidents'. The repository is public and has 551 stars, 32 forks, and 123 commits. The main content area displays the README file, which includes a 'Background' section. This section explains that the repository tracks publicly disclosed AWS customer security incidents with known root causes, excluding data store breaches and incidents already covered by other reports. It also notes that incidents impacting individuals are excluded. A 'Catalog of AWS Customer Security Incidents' table is partially visible at the bottom, with columns for Name, Date, Root Cause, Escalation Vector(s), Impact, and Link to details. The first row shows an impact of 50,000.

Name	Date	Root Cause	Escalation Vector(s)	Impact	Link to details
				50,000	Exclusive to Access

Three input fields are shown, each containing a word and a character count. The first field contains 'credential' (0/66), the second contains 'key' (1/41), and the third contains 'compromise' (1/40). Dotted lines connect these fields to the corresponding text in the repository's README.

<https://github.com/ramimac/aws-customer-security-incidents>

When Statistics are Actual Reality



The image shows a screenshot of a web article from Dark Reading. The header is dark red with the 'DARKREADING' logo on the left and navigation links 'The Edge', 'DR Tech', 'Sections', and 'Events' on the right. The article title is 'GitHub's Private RSA SSH Key Mistakenly Exposed in Public Repository' in bold black text. Below the title is a sub-header 'Application Security' with a clock icon, '1 MIN READ', and a 'QUICK HITS' icon. The author is 'Dark Reading Staff' with a circular profile picture and the date 'March 24, 2023'. The main image shows a laptop with the GitHub logo on the screen.

DARKREADING The Edge DR Tech Sections Events


Application Security | 1 MIN READ QUICK HITS

GitHub's Private RSA SSH Key Mistakenly Exposed in Public Repository

GitHub hastens to replace its RSA SSH host key after an exposure mishap threatens users with man-in-the-middle attacks and organization impersonation.

Dark Reading Staff
Dark Reading

March 24, 2023



"This week, we discovered that GitHub.com's RSA SSH private key was briefly exposed in a public GitHub repository. We immediately acted to contain the exposure and began investigating to understand the root cause and impact. We have now completed the key replacement, and users will see the change propagate over the next thirty minutes," [GitHub stated in the blog post](#).

GitHub replaced the RSA SSH host key to protect their users from the possibility that an adversary had seen the private key. Threat actors could use it to monitor users' operations or impersonate GitHub for follow-on attacks.

Use Cases to be Demonstrated



Reconnaissance

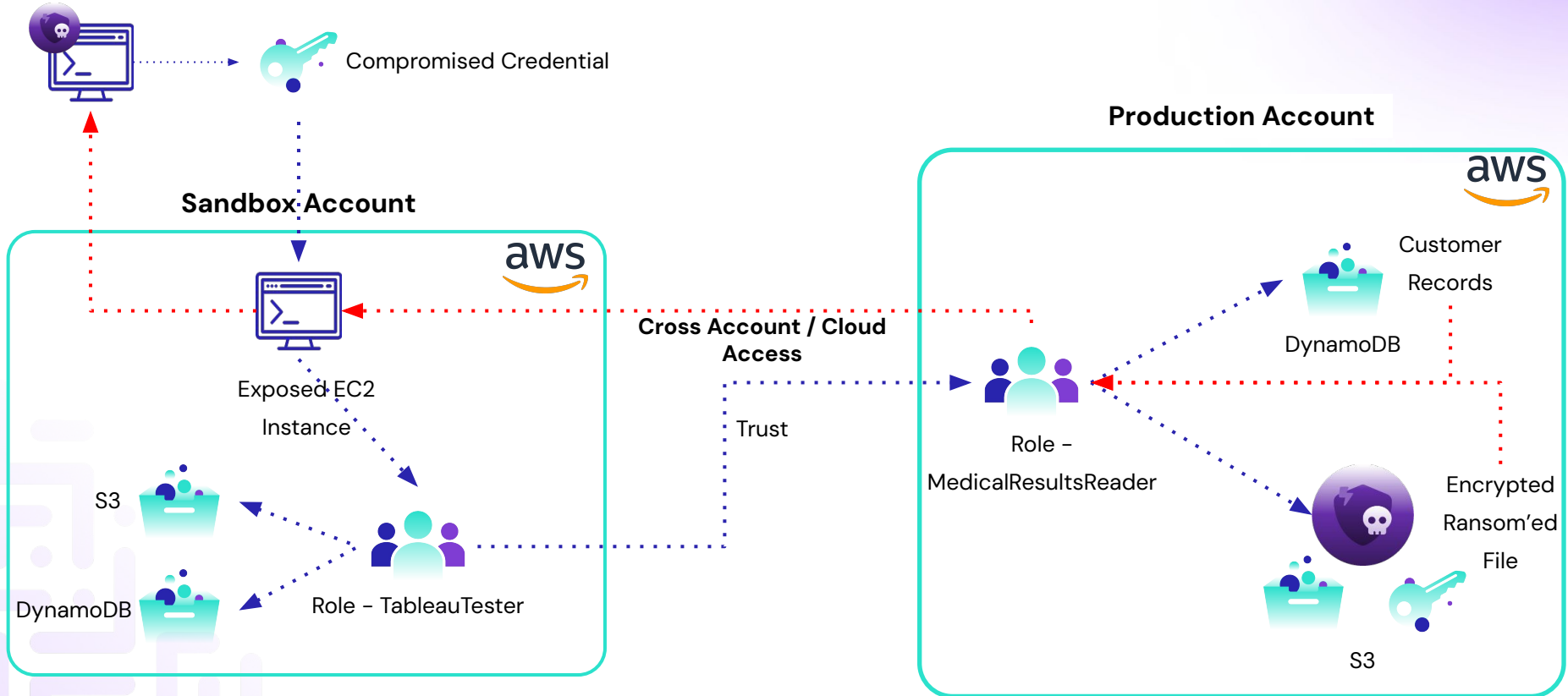
Lateral Movement

Privilege Escalation

Data Ransoming

Data Exfiltration

What You're About to See



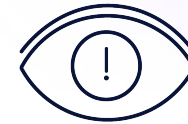
What Can You Do?



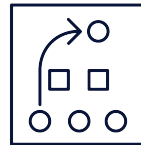
Carefully create and manage “break glass” identities



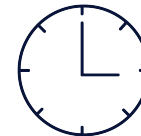
Have a team or process responsible to certify identities regularly



Kill dormant identities



Get to and maintain Least Privilege. Continuously monitor for Privilege Escalation risks



Continuously monitor your identities for behavior and/or permissions changes

Thank You

 <https://www.linkedin.com/in/jmoncrief/>