EA Games Credentials Leaked via Slack Cookies

Overview

In early June, Electronic Arts (EA) disclosed a data breach that resulted in hundreds of gigabytes of source code for various video games being stolen. Since then, it's been discovered that the attackers gained access to EA's infrastructure through stolen Slack cookies that contained login credentials belonging to employees. With those credentials, attackers were able to access certain Slack channels and pose as EA employees to the IT team to request a new MFA token and gain access to the organization's infrastructure. The group behind the attack claims they were able to repeat this process on two occasions.

Recommendation for Lookout Admins

Lookout administrators should be sure to leverage the granular Cloud Access Security Broker (CASB) access policies to prevent unauthorized logins and access to corporate infrastructure. These policies can be set up based user and device context such as the location they're logging in from and whether the action is taking place from a managed or unmanaged device. Implementing these policies can protect corporate SaaS apps and the data with them from being accessed by malicious or unauthorized users.

Lookout Analysis

Compromised user credentials are one of the biggest challenges for IT and security teams because an attacker can disguise themselves as a legitimate user and, as shown in this incident, pose as that user to IT to bypass security measures. Therefore, it's so important to have context-based login and access policies that can observe and baseline user behavior to detect anomalous activity such as an abnormal login location or massive data exfiltration. In addition, cloud services are so heavily integrated that attackers can move laterally through the infrastructure until they find the most valuable data they can exfiltrate.

Lookout Cloud Access Security Broker (CASB)

Lookout Cloud Access Security Broker (CASB) provides full visibility into the interactions between users, endpoints, cloud apps and your data. It also enables you to dynamically dial in Zero Trust access controls. With continuous monitoring of user and entity behavior analytics (UEBA), you can detect and respond to insider threats and advanced cyberattacks. We provide advanced data loss prevention that can classify, encrypt and restrict sharing of your data on the fly so that only authorized users have access.

Click here to learn more about Lookout CASB