HUMAN

BotGuard for Applications
Higher Education Case Study

Security Team, Ping and HUMAN Collaborate to Protect Single-Sign-On at a Leading University

1. The CISO at a leading US university was concerned that the student portal was under attack from sophisticated bots and that this could lead to a costly data breach.

2. By deploying a single line of code, Human BotGuard for Applications revealed that sophisticated bots had launched a sustained attack on the organization's single-sign-on page that guards more than 150 applications.

3. BotGuard was able to protect the portal single-sign-on (SSO) page from bots by integrating PingFederate with the Human Verification Engine adapter, greatly reducing development and implementation time and speeding up the time to protection.

CHALLENGE:

Uncovering Account Takeover

Account Takeover (ATO) attacks are one of the biggest challenges today in application security and the CISO of a leading US university suspected that their student portal was under attack from sophisticated bots.

The CISO approached HUMAN to help determine if his suspicions were correct, and if so, to assess the severity of the attack, the behavioral patterns, and add overall context to the fraud problem. To investigate, HUMAN engineers deployed the BotGuard tag in detection mode on the portal's SSO page.

Within a short period of time, HUMAN saw automated behavior indicating many credential stuffing and brute force attacks being used against the student portal SSO page. Alarmed by the large

proportion of bot traffic originating from known high fraud risk internet service providers, the HUMAN team updated the CISO immediately.

The university SSO page guards more than 150 applications. These critical applications are used by students to pay their tuition fees and bills, see their course schedules and update medical and other personally identifiable information (PII). With the risk of a costly or brand damaging breach looming large, an action plan needed to be developed quickly.

SOLUTION:

BotGuard for Applications

Implementing BotGuard to protect a single application requires minimal development work but implementing BotGuard in 150 applications authenticated by the same SSO page seemed a more considerable undertaking to the university security team.

However, the HUMAN solutions architect found a simpler answer. He noted that the university already used PingFederate, a leading identity and access management (IAM) solution, to enable user authentication and single-sign-on. PingFederate serves as a global authentication authority that allows university students, staff and partners to securely access all of the applications they need from any device. HUMAN partnered with the university security team and Ping to develop the Human Verification Engine adapter. This adapter captures signals created during a user authentication session and provides a decision to PingFederate on whether the end user is a verified human. This decision allows a PingFederate administrator to configure an authentication policy so that valid traffic is steered towards a frictionless option while malicious bot or automated traffic is steered towards 'access denied' or step-up authentication such as multi-factor authentication (MFA).

RESULTS:

Single Deployment, Maximum Protection

The university security team is currently protecting 30 custom-made applications with this integrated solution. By integrating PingFederate with the Human Verification Engine adapter on the portal SSO page, BotGuard now has the potential to protect all 150 applications from sophisticated bots with a single tag.

As minimal further development effort is needed, the team plans to protect the remaining 120 third-party software-as-a-service applications accessed from the student portal, greatly speeding the time to protect the remaining applications.

The university now has a tightly-integrated identity and bot management solution. Integrating PingFederate with BotGuard for Applications now protects the university's web and mobile applications from threats such as account takeover (ATO), credential stuffing, credential cracking, new account creation, content abuse and payment fraud.