PROTECT YOUR UNICORN FROM HUNTERS

Nir Valtman
Chief Information Security Officer
WHO IS KABBAGE?
A STORY ABOUT TRANSFORMATION
INFO SEC PROGRAM FOUNDATIONS

• PEOPLE
• PROCESS
• TECHNOLOGY
THIS IS HOW I FELT WHEN JOINED KABBAGE
BUT THEN I REALIZED...
TOWNHALLS & TECH ALL HANDS
UNLOCKED SCREEN
PRANKS

1. lets try this again
   i am a poopy butt

2. Kabbage
   1:22 PM
   https://i.giphy.com/media/M4Ru0rxfXwhSo/giphy.gif (123 kB)

3. persistence is key
INFO SEC PROGRAM FOUNDATIONS

• PEOPLE
• PROCESS
• TECHNOLOGY
COMPLIANCE  SECURITY
BECOME A BUSINESS ENABLER

Source: https://vignette3.wikia.nocookie.net/matrix/images/0/0d/Tank_Meets_Neo.png
KaBounty, an internal security bounty program

What is a bug bounty program?
A bug bounty program, also called a vulnerability rewards program (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs. Many software vendors run bug bounty programs, paying out cash rewards to software security researchers who report software vulnerabilities that have the potential to be exploited.

What is KaBounty?
KaBounty is similar to the traditional bug bounty program, but it has its own twist. As opposed to accepting vulnerability reports from individual security researchers across the world, we decided to adjust the program as follows:
- We don’t restrict the program to only reporting software vulnerabilities. You can also report almost any sort of problem: IT asset misconfiguration, improper process implementation that can be exploited, or any other vulnerabilities that may affect Kabbage’s security posture.
- This program is for Kabbage employees only; independent security researchers are not eligible at this time.

Rewards
A reward is given to a sole submitter if the reported vulnerability is new to the information security team.

The provided rewards are based on the security risk: the higher the risk, the higher the reward:

<table>
<thead>
<tr>
<th>Risk Severity</th>
<th>Reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>$</td>
</tr>
<tr>
<td>Medium</td>
<td>$</td>
</tr>
<tr>
<td>Low</td>
<td>$</td>
</tr>
<tr>
<td>Informational</td>
<td>Kudos</td>
</tr>
</tbody>
</table>

KaBounty HALL OF FAME
Beyond the monetary reward, we’d like to share with everyone the status of the program at any given time.

Below is the list of the hall of fame:

<table>
<thead>
<tr>
<th>Name</th>
<th>Total Rewards ($)</th>
<th>Valid Submissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$</td>
<td></td>
</tr>
</tbody>
</table>

How to report a vulnerability?
It’s a simple 3-step process:
1. Think.
2. Think Again.
3. Fill the form below.

Summary
* e.g. unauthorized users are exposed to PII via AppX

How did you discover the problem?
*
INFO SEC PROGRAM FOUNDATIONS

- PEOPLE
- PROCESS
- TECHNOLOGY
TECH CLASSIFICATION ON YEAR 1

- SAST
- DAST/IAST
- Software Composition Analysis
- Containers
- WAF/RASP
- Vulnerability Scanning
- Secret Management
- MFA
- Network Segmentation
- EDR
- DLP/CASB
- MFA
- Ammmmm... ?

TRAINING

SIEM/SOC

PRIVACY
UTILIZE EXISTING TOOLS
 WHICH COMPANY IS MORE LIKELY TO PURCHASE A SOLUTION FROM A STARTUP?
HOW TO PROTECT YOU UNICORN FROM HUNTERS?

IT SHOULD NOT LOOK LIKE THIS
HOW TO PROTECT YOUR UNICORN FROM HUNTERS?

BUT MORE LIKE THIS

Source: https://www.deviantart.com/sandara/art/black-mountain-unicorn-368791768
Questions?