CORPSEC: WHAT HAPPENED TO CORPSES A AND B?

Chris Czub
Senior Information Security Engineer
Duo Security
@chrisczub
What is Corpsec Engineering?

- Corpsec Engineering’s Purpose: prevent and detect threats at Duo as we scale
- We have engineering resources
- You can do this too
- You don’t need a full staff of 7 engineers to do all of this
Corpsec Engineering Responsibilities

- Eat our own dogfood: Duo Beyond
- Manage endpoints
  ~600 MacOS endpoints, ~200 Chromebooks, ~10 Windows
- Manage internal security services and applications
- Cloud service security
- Employee security education and support
Corpsec Motivations

- Scaling
- Enabling business
- Securing employees
- Building internal trust
Corpsec Goals

- Visibility
- Consistency
- Trust
- Preventing compromise
Corpsec Engineering Programs

- Detection Engineering
- Endpoint Detection and Response
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics
StreamAlert
Why StreamAlert?

- Scalable — just add more shards
- Actively developed
- Rules as code
- Unit Testable
- Supports many data sources/outputs/types
Why NOT StreamAlert

- Rigid
- Difficult to debug
- Hard to test end-to-end locally
- Stateless (for now)
- Need engineering support to deploy and develop on
- No correlation
Lessons Learned

- StreamAlert is *not* log aggregation or SIEM
- Will require legwork to customize for your needs
- ChatOps gets noisy fast
- Need feedback loop for alerts
  In our case, we feed them back to our SOA platform
Corpsec Engineering Programs

- Detection Engineering
- **Endpoint Detection and Response**
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics
Endpoint Detection and Response
Problem statement

- We need to have an anti-malware strategy for endpoints
- Application whitelisting is one of the most effective ways to prevent malware, but can be a nightmare to deploy without annoying your users
- We wanted to cover the vast majority of malware cases with the least expense
- We wanted to leverage threat intelligence sources to enable detection after the fact
OS X App Whitelisting That Won’t Get You Fired

- Santa from Google
- Open source
- Imperfect
- No built-in server-side component
Santa

The following application has been blocked from executing because its trustworthiness cannot be determined.

<table>
<thead>
<tr>
<th>Filename</th>
<th>010 Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>/Applications/010 Editor.app/Contents/MacOS/010 Editor</td>
</tr>
<tr>
<td>Publisher</td>
<td>SweetScape Software Inc. - Developer ID Application: SweetScape Software Inc. (252VCA66Z8)</td>
</tr>
<tr>
<td>Identifier</td>
<td>5a6dc8a23f9a0975d8530f3e470086c0b55d1f5ca8e62bdacbc4ecdec6b326c6c9</td>
</tr>
<tr>
<td>Parent</td>
<td>launchd (1)</td>
</tr>
<tr>
<td>User</td>
<td>chris</td>
</tr>
</tbody>
</table>

- Prevent future notifications for this application for a day

Ignore
Santa Deployment Strategy

- **Weeks 1-4:** Deploy in monitor mode, collect data
- **Week 5:** Generate initial whitelist
- **Weeks 6-10:** Add pilot groups to enforcing mode, collect feedback
- **Weeks 11-15:** Find better solution than analyst manual whitelisting (self-service in our case) and automate
- **Weeks 16+:** Full deployment
ChatOps Whitelisting

- We used our SOA system (Komand) and some custom code to create a self-service whitelisting flow in Slack

Security Bot: Hey cczub! We noticed that something was blocked from running on your machine.

Our goal is to keep you safe, while enabling you to do your job.

Please direct any questions about this to #santa-support-group

Did you mean to run the application 010 Editor

(/Applications/010 Editor.app/Contents/MacOS)?

If you select 'yes', you will be able to run it after performing a sync (santactl sync).

Yes  No
ChatOps Whitelisting

- We used our SOA system (Komand) and some custom code to create a self-service whitelisting flow in Slack

---

Security Bot  APP  11:50 AM
Okay! This application (010 Editor) has been whitelisted. Your machine should automatically sync Santa rules within the next 30 seconds and you can try running the application again! If you have any problems, please visit #santa-support-group and my team of humans would be happy to help, under threat of battery removal.
A Look At the Naughty List

- 268 whitelisted developer certificates
- 1238 whitelisted binary hashes
- 20000+ application launches analyzed per week
- Dozens of potentially unwanted applications blocked
Santa Infrastructure

- A server-side component to maintain the whitelist
- A front-end for managing the whitelist (adding, removing, and auditing)
- Configuration management to set the endpoints up
- Orchestration and automation
- Log forwarder from Santa to log management
- Log forwarder from Santa to orchestration platform
- Something to perform periodic checks of whitelist (scheduled Lambda)
Results

- Detected potentially unwanted apps and malware
- Deployed in four months in enforcing mode... without losing our jobs
- Freed up resources to focus on more sophisticated threats
- Quick, automated turnaround from detection to remediation for garden-variety malware and PUAs
OSQuery

Facebook's Open-Source Security Tool

Windows / Mac OS X / Linux
OSQuery and Kolide Fleet

- Open source
- Indicator-based compromise and anomaly detection
- Real-time querying
- Tagging so we can query subgroups
- Slick web UI
- Scheduled Queries
Edit Query

Query Title
All LaunchDaemons

SQL
1 SELECT * FROM launchd

Description
Select all LaunchDaemons

SAVE

Select Targets
Label Name, Host Name, IP Address, etc.

RUN

0 unique hosts

Choose a Table

users
Local system users.

OS Availability
All Platforms

Columns
uid big int
uidSigned big int
gid big int
gidSigned big int
username text
description text
directory text
shell text
uuid text
Corpsec Engineering Programs

- Detection Engineering
- Endpoint Detection and Response
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics
Security Orchestration and Automation

- A few big players here
- We went with Komand
- Hundreds of pre-built integrations
- Reusable components
- Easy to script for in Python/Golang
- Visual flowcharts are easy artifacts to explain and display
<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Last Edited</th>
<th>Steps</th>
<th>Decisions</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFPIO Processing v1</td>
<td>04/09/18</td>
<td>6</td>
<td>1</td>
<td>no tags</td>
</tr>
<tr>
<td>Automated Password Alert Dev</td>
<td>04/09/18</td>
<td>28</td>
<td>2</td>
<td>no tags</td>
</tr>
<tr>
<td>Securitybot Slack DM Outgoing Messenger</td>
<td>04/09/18</td>
<td>8</td>
<td>1</td>
<td>slack, gmail, email</td>
</tr>
<tr>
<td>StreamAlert</td>
<td>03/30/18</td>
<td>6</td>
<td>0</td>
<td>no tags</td>
</tr>
<tr>
<td>VulnMgmt v2</td>
<td>03/30/18</td>
<td>15</td>
<td>2</td>
<td>no tags</td>
</tr>
<tr>
<td>OmnitzaChefWorkflow</td>
<td>03/29/18</td>
<td>3</td>
<td>0</td>
<td>no tags</td>
</tr>
<tr>
<td>BetaBot</td>
<td>03/27/18</td>
<td>7</td>
<td>0</td>
<td>slack, gmail, email</td>
</tr>
<tr>
<td>Santa Whitelist</td>
<td>03/23/18</td>
<td>17</td>
<td>2</td>
<td>no tags</td>
</tr>
</tbody>
</table>
Corpsec Engineering Programs

- Detection Engineering
- Endpoint Detection and Response
- Automation and Orchestration
- Corporate Application Security
- DevOps
- Employee Education
- Data Analytics
Engineered Employee Education

- Enlighten — gamified security
- SecurityBot — a trusted Slack bot for comms and interactions
- Phishing campaigns
- OAuth phishing
Who Is SecurityBot?

- A little bit of all of the above...

Securitybot, 1260316800

I enjoy long rolls on the beach, traveling, hanging out with my bestie Johnny 5, and of course - making security easy at Duo!
Whatcha Thinkin’ About, SecurityBot?

- Santa Notifications
- Beta Program Invitations
- Password Alert Messaging
- Messages from the Security Team
- A Source of Trusted Information and True Facts #nophish
Hey there! As part of our continued efforts to own the Beyond market opportunity and elevate the security story internally at Duo, the Security department is launching a lightweight monthly newsletter. This is our first attempt to start communicating more frequently with the broader team where our focus is in the Security department in key areas: research and development in Labs, Application Security work to help ship safe and secure software, and our Corporate Security efforts to defend our internal systems and data in a positive and progressive fashion. We hope you like it, and we welcome your feedback on what you'd like to see next month!

Click here to read the newsletter
Hi asturdevant,

The CorpSec team is requesting your help to test a new product/feature. If you decide to help, you can join the channel: #corpsec where you can ask questions and get help, if needed. We understand if you're too busy to help with a beta feature right now, you can also click, *Sorry, not now,* or simply ignore me to *opt-out* of this invitation. Below is a quick description of the product/feature that the CorpSec needs help testing.

Description:
Hello! This is a sample beta program enrollment from Security Bot!

Would you like to participate?

Awesome, Yes!  Sorry, not now.
Hi there, iOS 11.2.6 has only been out for one day and you've already updated! 🎉 Thanks for keeping Duo secure.
Hello! I am Security Bot and I have a new feature! 🪤

Starting today, if you accidentally type your Duo Google account password in another website, I will provide an easy prompt to help you change your password. I will also double check to see if the website is potentially malicious, if so I will let you know and help you change your password immediately.

Don't hesitate to reach out to security@duosecurity.com or the #security slack channel with any questions!
Questions?