CYBERARK

ATTACK & DEFEND SERIES

MAJOR BREACH EDITION

LEGAL DISCLAIMER

This presentation contains materials that can be potentially damaging or dangerous.

These materials are for educational and research purposes only.

All tools provided are open source and CyberArk is not associated with any tools provided. Do not attempt to violate the law with anything contained here. If this is your intention, then **LEAVE NOW!** Neither the authors of this material, CyberArk, or anyone else affiliated in the content in any way, is going to accept responsibility for your actions.

We promote hacking, but do not promote CRIME! We are documenting the ways criminals steal and perform their nefarious acts, so you can defend yourself and your organization.

ANDY THOMPSON

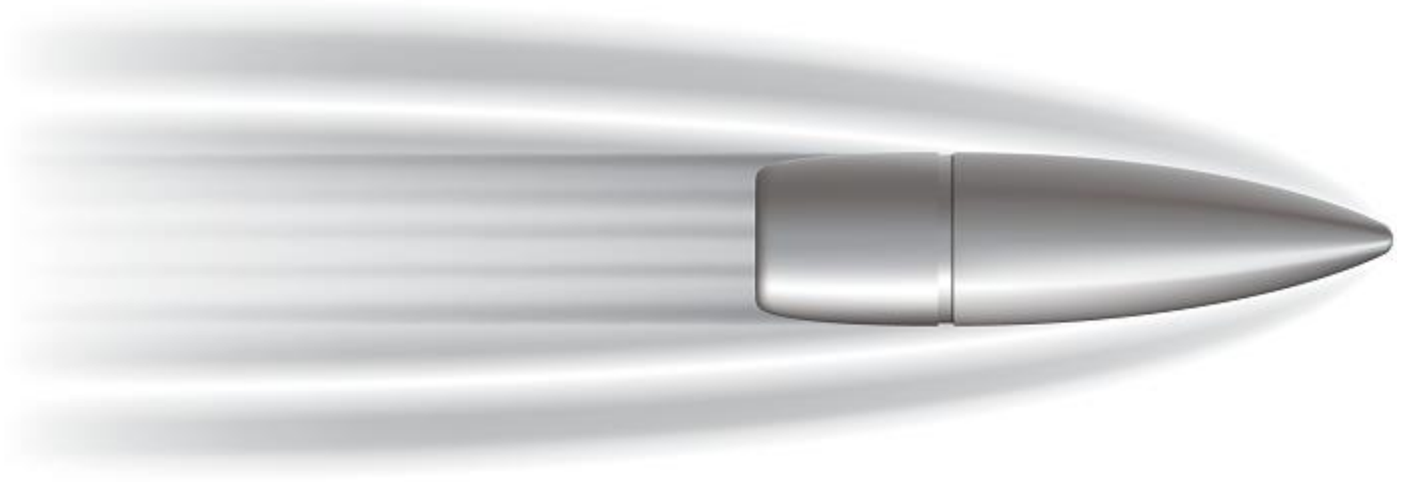
Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

- Global Research Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hacker
- Travel-Hacker

THE SILVER BULLET

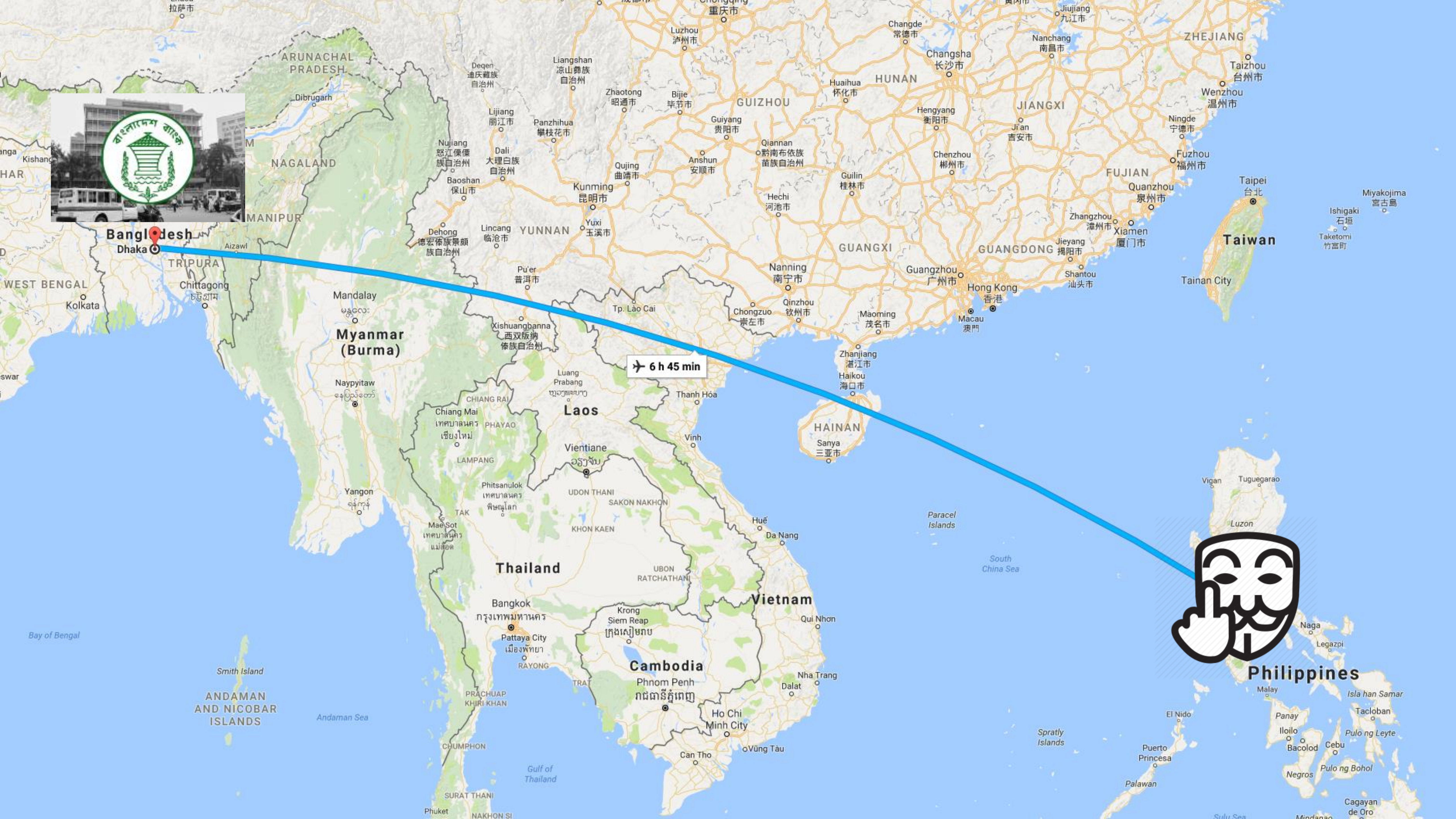
- There is **no** silver bullet.
- CYBR will buy invaluable time.
- Detecting attacks earlier.
- Preventing attackers from theft or disruption.



MAJOR BREACH EDITION

Each section will include:

- Case Study.
- Attack Demo.
- CYBR Response.



6 h 45 min
Bangladesh
Dhaka
Kolkata
WEST BENGAL
Chittagong
TRIPURA
Aizawl
MANIPUR
NAGALAND
ARUNACHAL PRADESH
Dibrugarh
Kishang
Myanmar (Burma)
Mandalay
Naypyitaw
Yangon
Bay of Bengal
Andaman Sea
Smith Island
ANDAMAN AND NICOBAR ISLANDS
Thailand
Chiang Mai
CHIANG RAI
PHAYAO
LAMPANG
Phitsanulok
TAK
Mae Sot
UDON THANI
SAKON NAKHON
KHON KAEN
UBON RATCHATHANI
Bangkok
Pattaya City
RAYONG
PRACHUAP KHIRI KHAN
CHUMPHON
SURAT THANI
Phuket
NAKHON SI
Gulf of Thailand
Laos
Luang Prabang
Vientiane
Cambodia
Krong Siem Reap
Phnom Penh
TRAT
Vietnam
Tp. Lào Cai
Thanh Hóa
Vinh
Huế
Da Nang
Qui Nhon
Nha Trang
Dalat
Ho Chi Minh City
Vũng Tàu
Can Tho
YUNNAN
Kunming
Dali
Lijiang
Deqen
Nujiang
Baoshan
Dehong
Lincang
Pu'er
Xishuangbanna
Yuxi
Qujing
Zhaotong
Liangshan
Panzhihua
Bijie
GUIZHOU
Guiyang
Anshun
Qiannan
Luzhou
Chongqing
GUANGXI
Nanning
Hechi
Guilin
Chongzuo
Qinzhou
HUNAN
Huaihua
Changde
Changsha
Hengyang
Chenzhou
JIANGXI
Nanchang
Jiujiang
Ji'an
GUANGDONG
Guangzhou
Hong Kong
Macau
Maoming
Zhanjiang
Haikou
HAINAN
Sanya
Shantou
Jieyang
FUJIAN
Fuzhou
Ningde
Quanzhou
Xiamen
Zhangzhou
ZHEJIANG
Wenzhou
Taizhou
Taiwan
Taipei
Tainan City
Miyakojima
Ishigaki
Taketomi
Paracel Islands
South China Sea
Spratly Islands
Philippines
Luzon
Vigan
Tuguegarao
Naga
Legazpi
Malay
Isla han Samar
Tacloban
Pulo ng Leyte
Panay
Iloilo
Bacolod
Cebu
Negros
Pulo ng Bohol
El Nido
Puerto Princesa
Palawan
Cagayan de Oro
Sulu Sea

CASE STUDY

- Attempted theft of $951 million
  - $851 million flagged by NY Fed
  - $20 million to Sri Lanka
  - $80 to the Philippines

- **US$63 million stolen.**
  - **Largest bank heist ever.**

ATTACK BREAKDOWN

- Adversary compromised initial system.
  - Elevated permission to Domain Admin.
- Executed Golden Ticket Attack.
- Pivot to Swift network segment.
  - Processed fraudulent transactions.

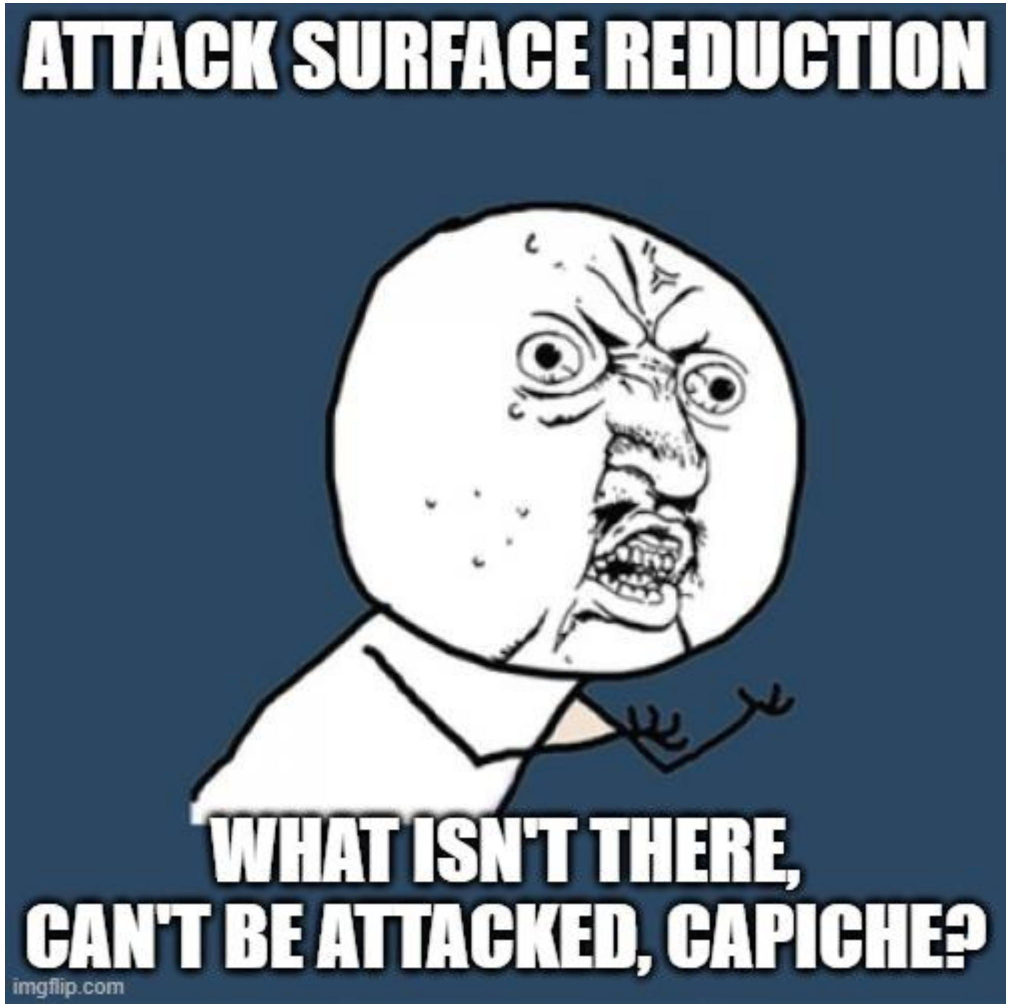
RECORDED ATTACK DEMO

DEFENSE BREAKDOWN

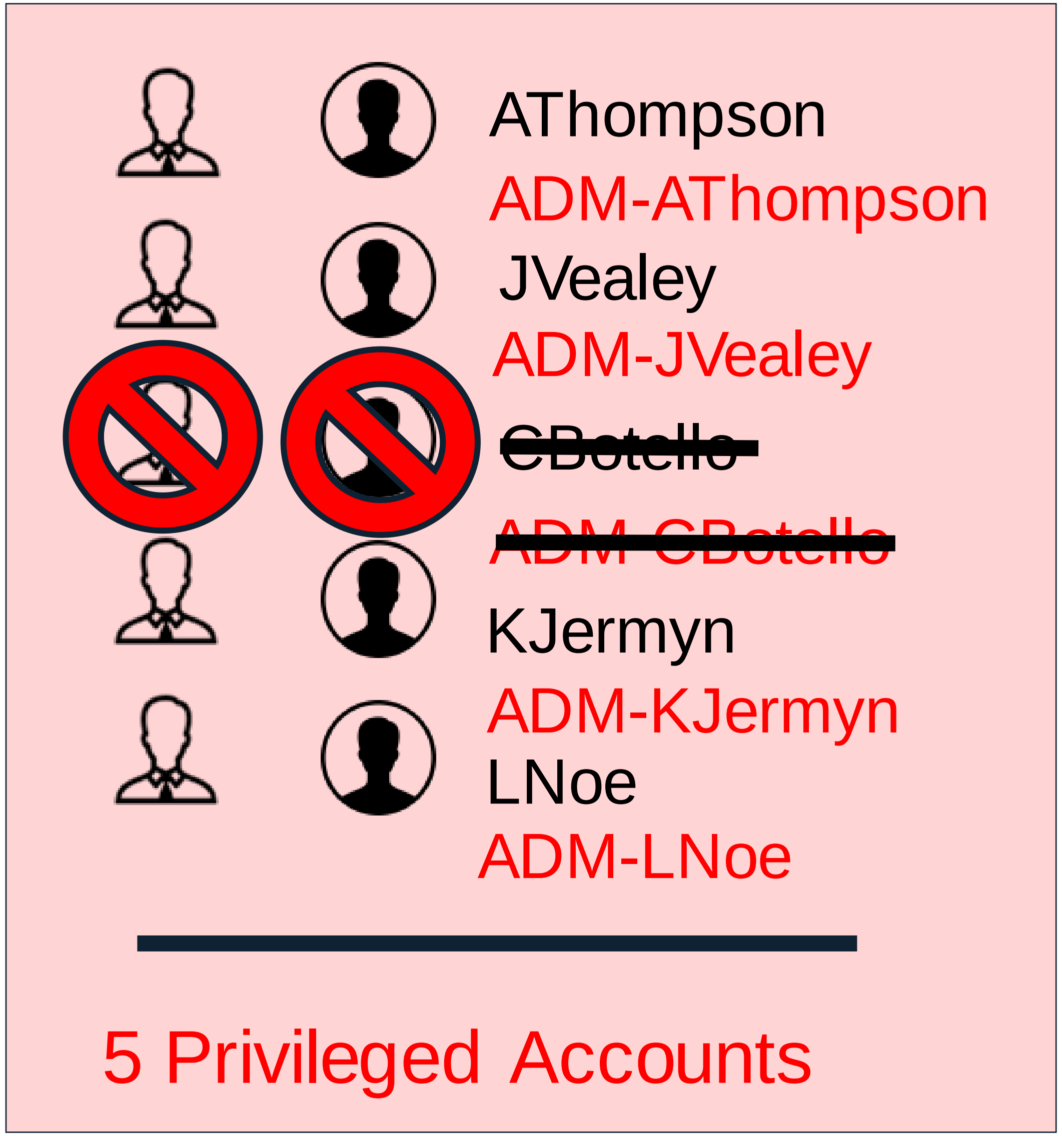
- Prevent the initial compromise with Endpoint Privilege Manager.
- Detect anomalous behavior & alerting with Privilege Threat Analytics.
- Protect the privileged credentials through credential boundaries and Privileged Session Management.

ATTACK SURFACE REDUCTION

- Reduce surface area by removing/disabling unused or unnecessary applications and service principals.
- Reduce permissions on applications and service principals, especially application permissions.
- Reduce the number of users that are members of highly privileged Directory Roles, like Global Administrator, Application Administrator, and Cloud Application Administrator.



ROLE-BASED ACCESS CONTROL



AThompson

ADM-AThompson

JVealey

ADM-JVealey

~~CBotello~~

~~ADM-CBotello~~

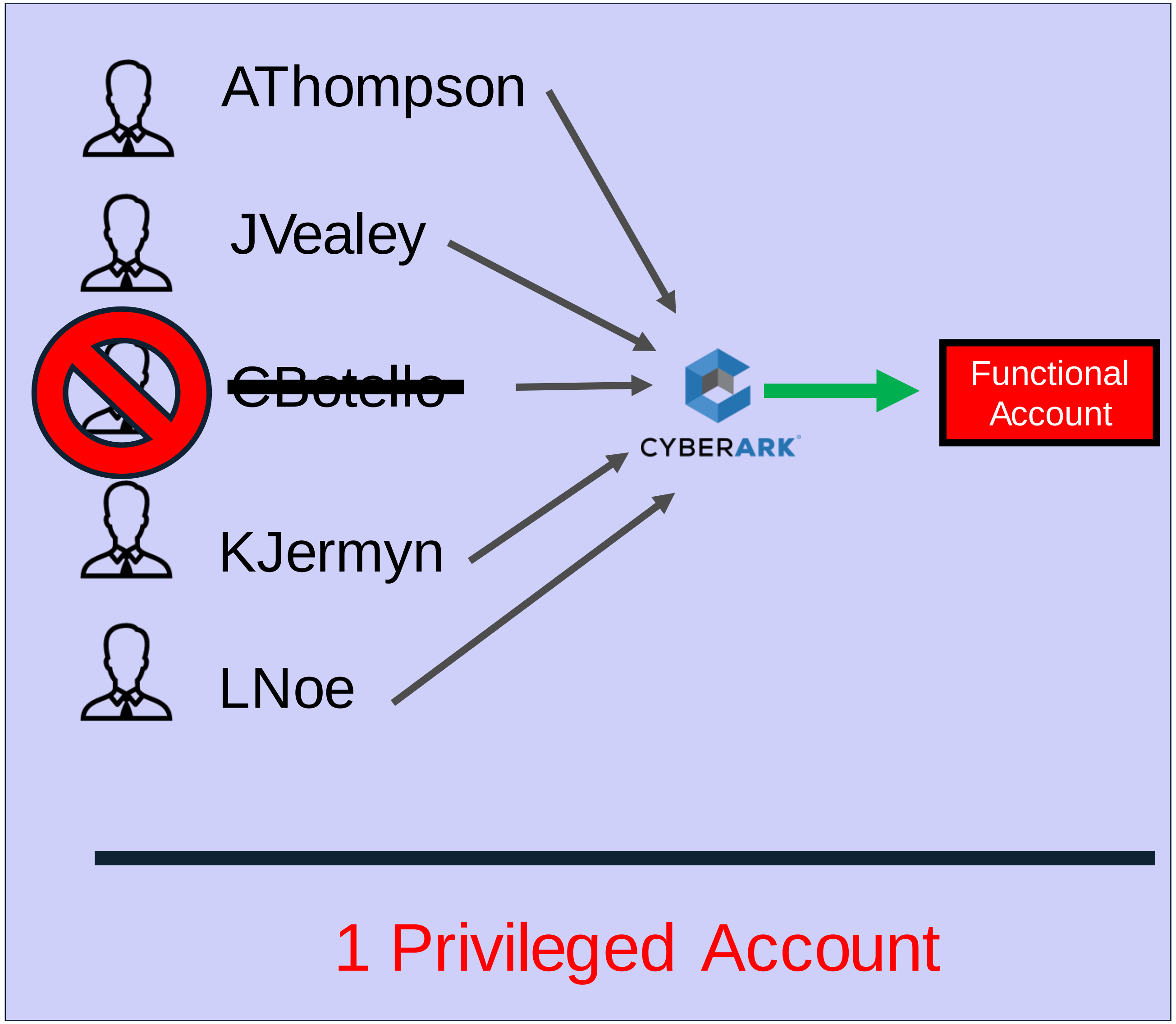
KJermyn

ADM-KJermyn

LNoe

ADM-LNoe

5 Privileged Accounts



AThompson

JVealey

~~CBotello~~

KJermyn

LNoe

Functional Account

1 Privileged Account

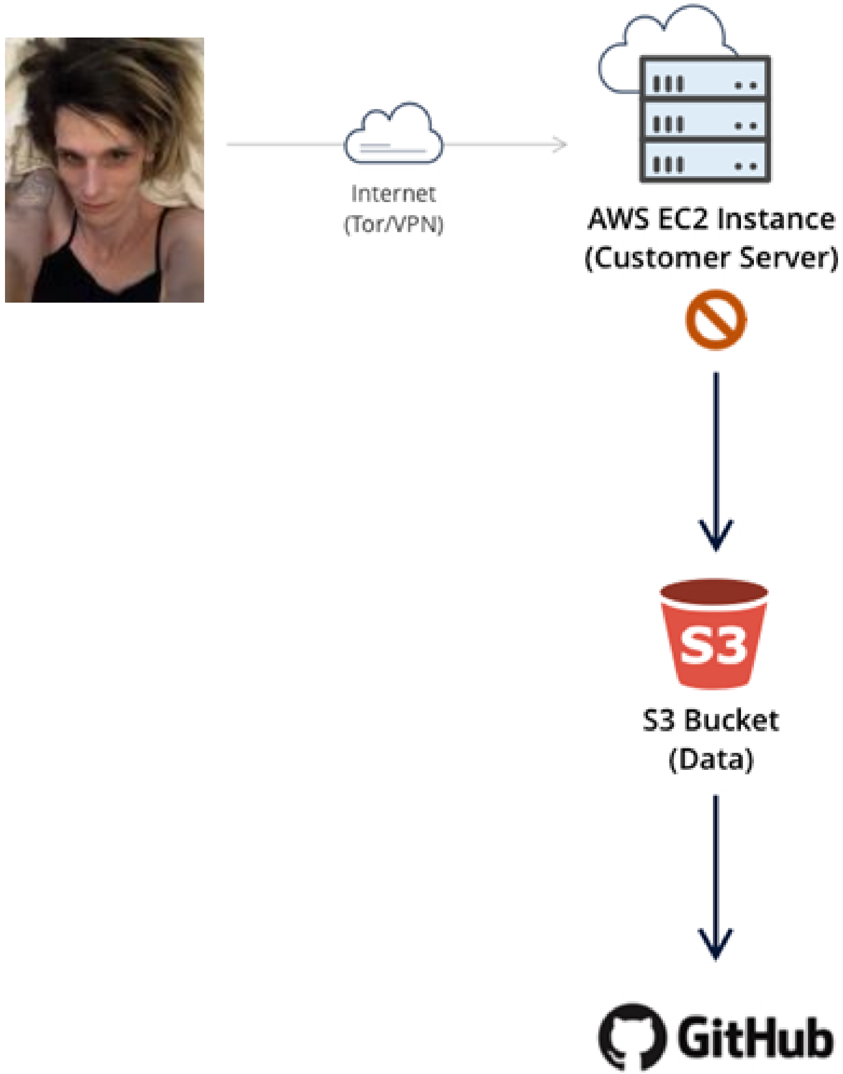
LARGE FINANCIAL INSTITUTION

[NAME REDACTED]

CASE STUDY

- 140,000 US Social Security Numbers
- 1,000,000 Canadian Social Insurance Numbers
- 80,000 bank account numbers
- Customer Information
  - Names
  - Addresses
  - Credit Scores
  - Bank Balances
  - And more!

CAPITAL ONE DATA BREACH



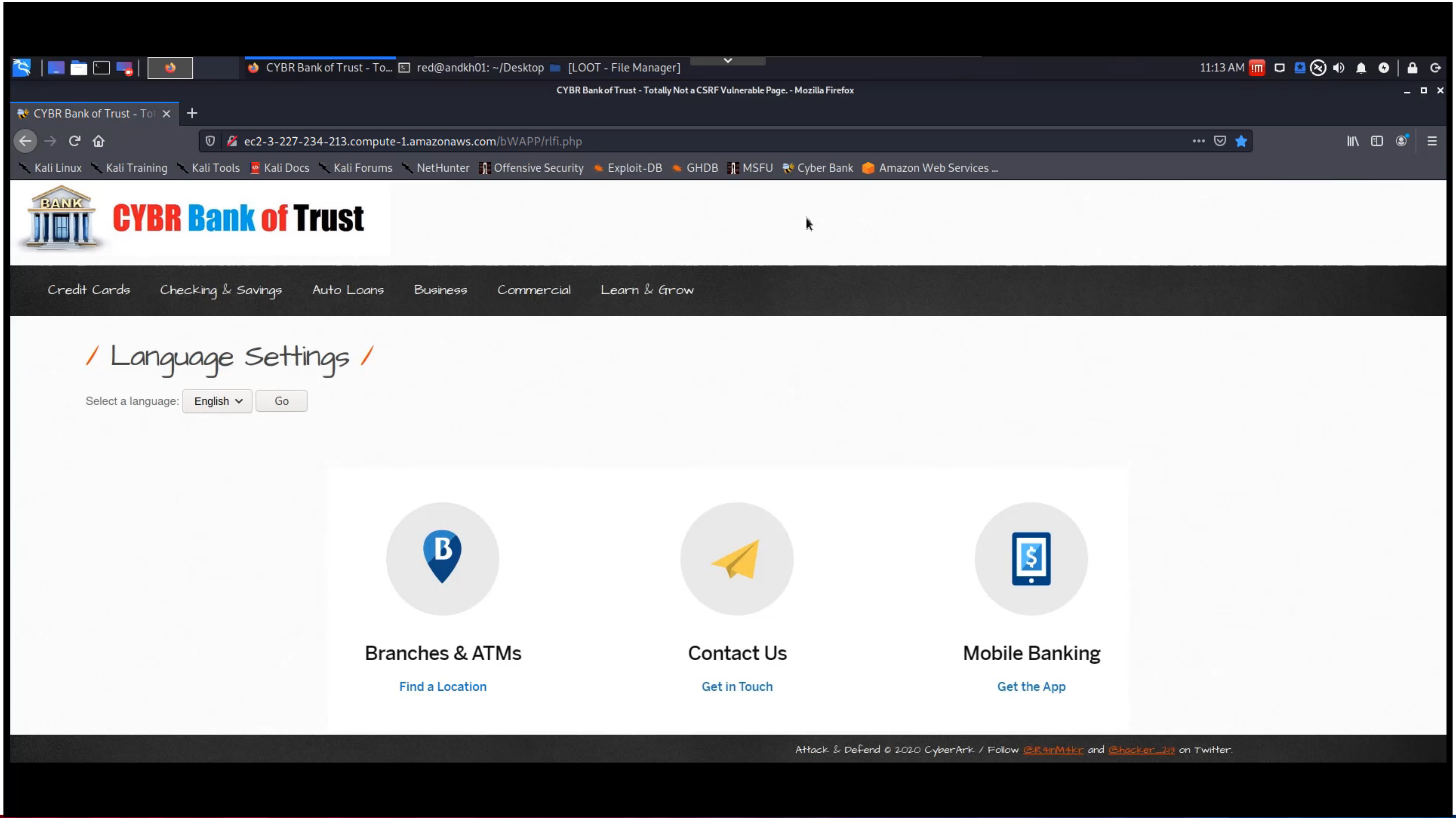
PART ONE

1. *Attacker’s IP address allowed to connect. (Firewall misconfiguration)*
2. *Exploit SSRF vulnerability of NGINX.*
3. *Access EC2 instance metadata.*

PART TWO

1. Assumed Role *****-WAF-Role
   (Role Permission Misconfiguration)
2. Execute Commands:
   - ListBucket:
     This permission shouldn’t be allowed for the WAF-Role
   - SyncBucket
     Last execution for that Role > 7 months.

RECORDED ATTACK DEMO



/ Language Settings /

Select a language: English Go

Branches & ATMs

Find a Location

Contact Us

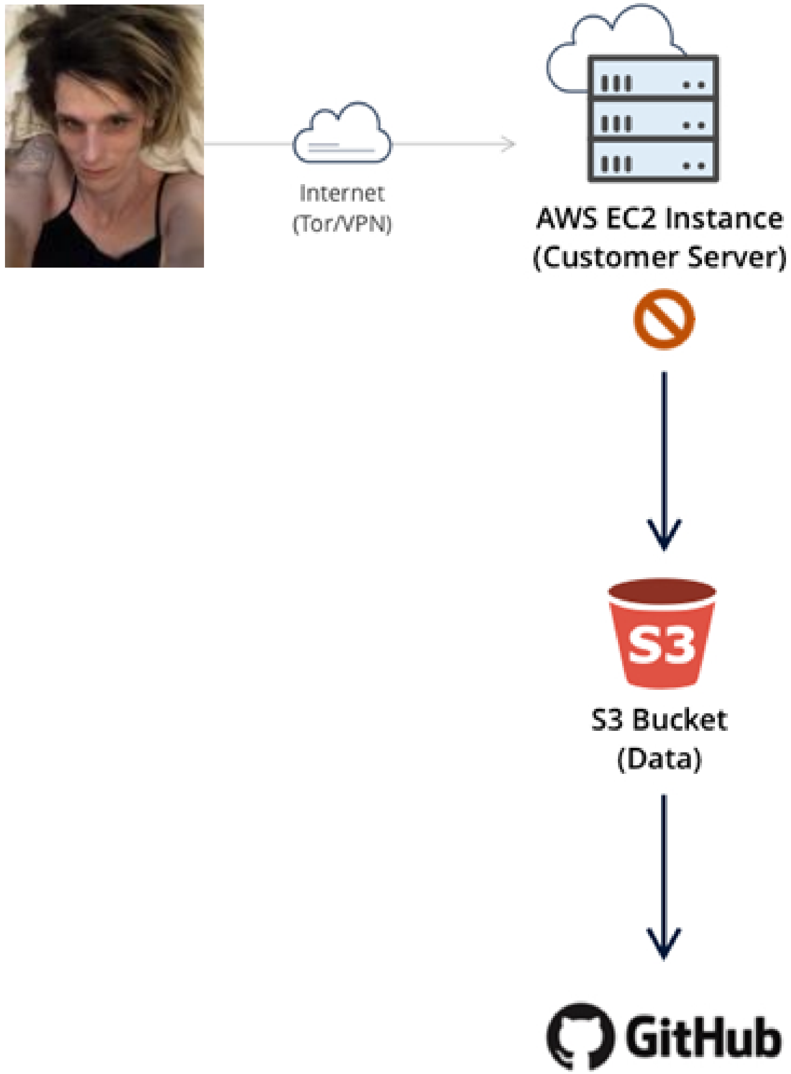
Get in Touch

Mobile Banking

Get the App

Attack & Defend © 2020 CyberArk / Follow @R4inM4kr and @hacker_213 on Twitter.

CAPITAL ONE DATA BREACH



1. Attacker's IP address allowed to connect (Firewall misconfiguration)
2. Assumed Role *****-WAF-Role
   (Role Permission Misconfiguration)
3. Execute Commands:
   - ListBucket:
     This permission shouldn't be allowed for the WAF-Role
   - SyncBucket
     Last execution for that Role > 7 months.

CyberArk can:

- Detect and Alert on excessive permission of the WAF-Role
- Clean up unused permissions
- Apply Least Privilege
- Block the attack early
- **With ZERO footprint and 5-minute setup.**

HOW CAN CYBERARK HELP?

- **RBAC to AWS**
  - ➢ Reduces attack surface and easier management of roles.
- **Detection and onboarding with Privilege Threat Analytics**
  - ➢ AWS integration and management with EPV/PSM
- **Cloud Entitlements Manager**

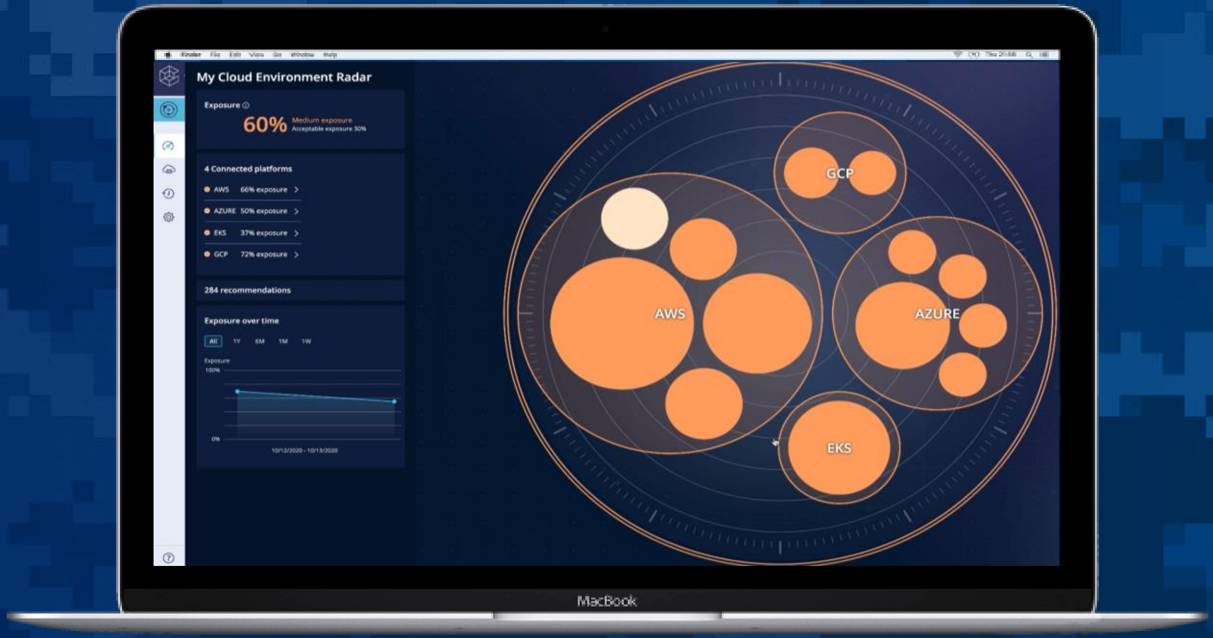
CLOUD ENTITLEMENT MANAGER

CEM a SaaS solution that reduces risk by implementing the Principle of Least Privilege in multi-cloud environments.

CEM centralizes visibility and control of permissions across an organization’s cloud estate.

By:

- Analyzing granted permissions.
- Identifying unused and excessive permissions.
- Modeling exposure level.
- Actionable recommendations.
- Deployable remediations.



My Cloud Environment Radar

Exposure ⓘ

60% Medium exposure
Acceptable exposure 30%

4 Connected platforms

- AWS 66% exposure >
- AZURE 50% exposure >
- EKS 37% exposure >
- GCP 72% exposure >

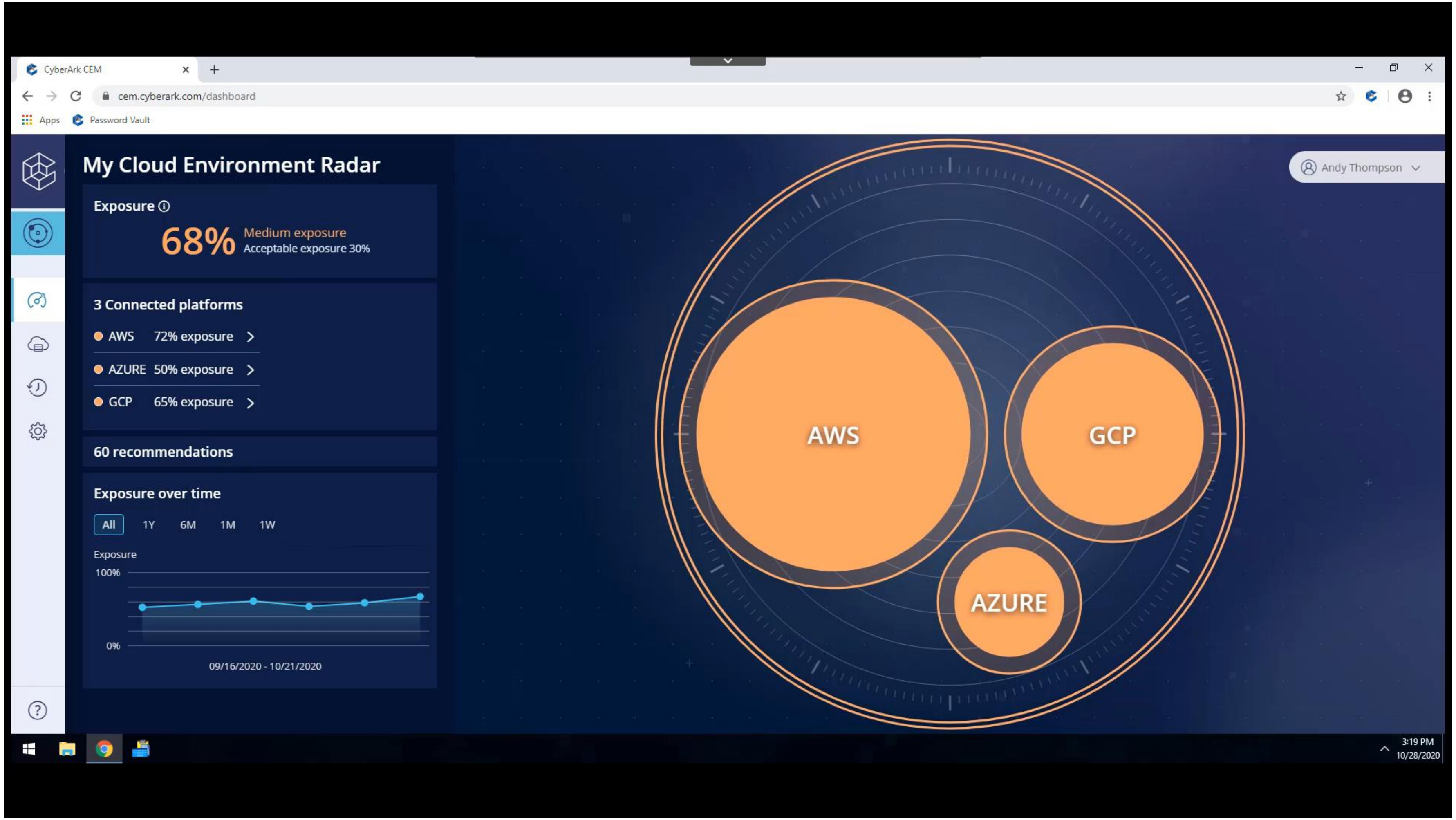
284 recommendations

Exposure over time

All 1Y 6M 1M 1W

Exposure
100%
0%
10/12/2020 - 10/13/2020

RECORDED DEFENSE DEMO



My Cloud Environment Radar

Exposure ⓘ

68% Medium exposure
Acceptable exposure 30%

3 Connected platforms

- AWS 72% exposure >
- AZURE 50% exposure >
- GCP 65% exposure >

60 recommendations

Exposure over time

All 1Y 6M 1M 1W

Exposure
100%
0%
09/16/2020 - 10/21/2020

SOLAR WINDS

CYBERARK®

CASE STUDY

Solar Winds

- Dec 8th, FireEye breach. Red Team tools leaked.
- SolarWinds Orion was the initial foot-hold.
- Attribution points to APT.

SOLARWINDS ATTACK CHAIN

STAGE 1

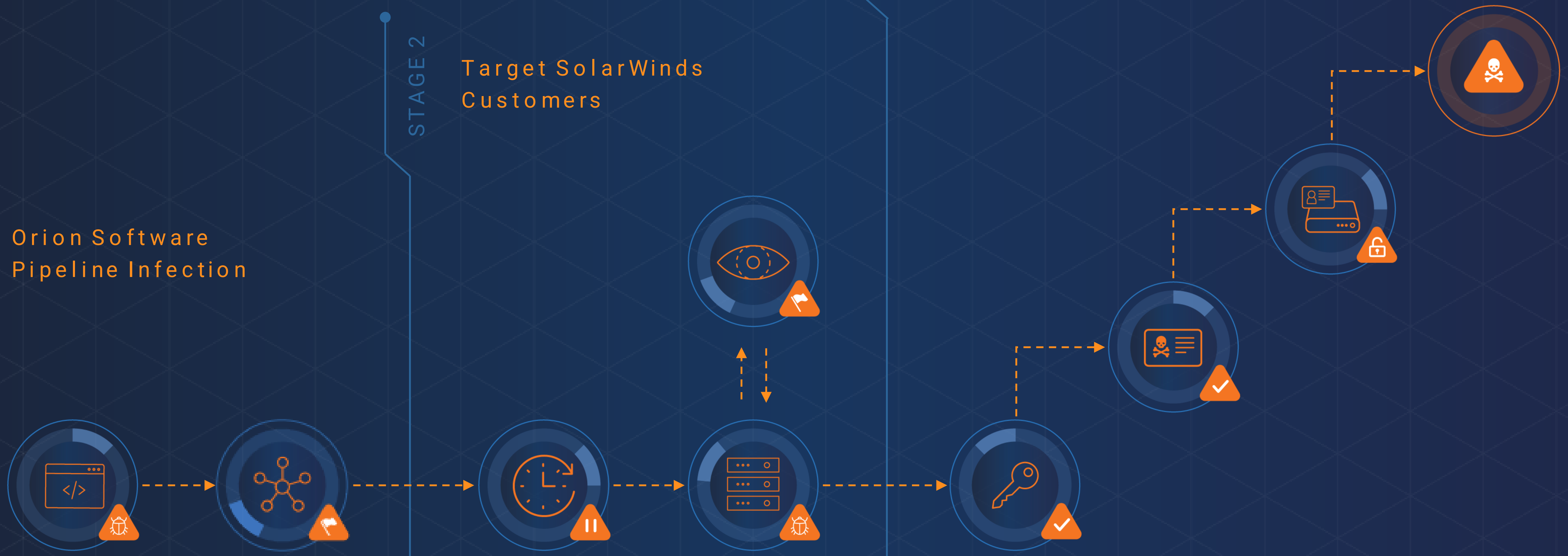
Orion Software
Pipeline Infection

STAGE 2

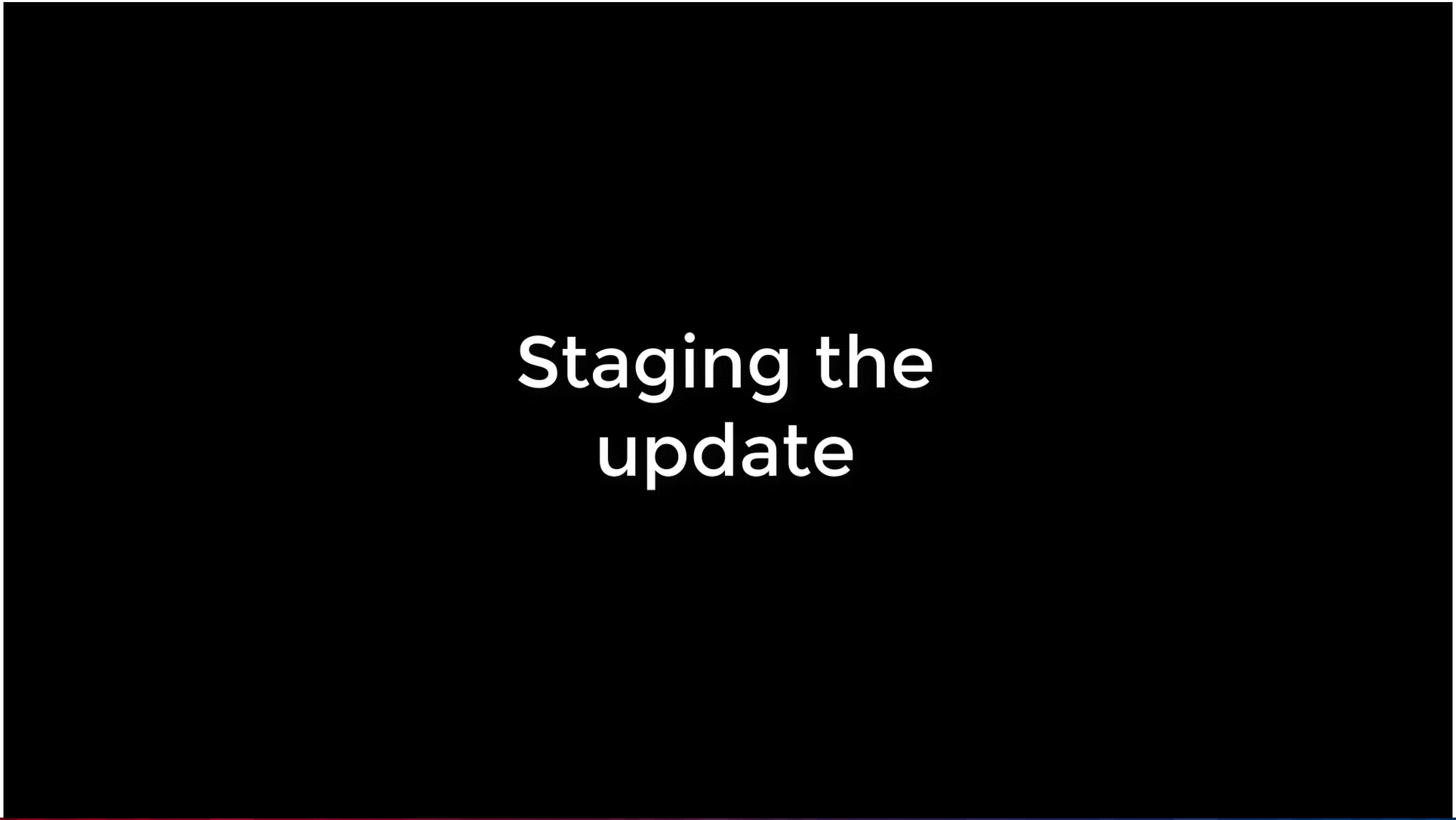
Target SolarWinds
Customers

STAGE 3

Privilege Escalation
to High Value Assets



RECORDED ATTACK DEMO

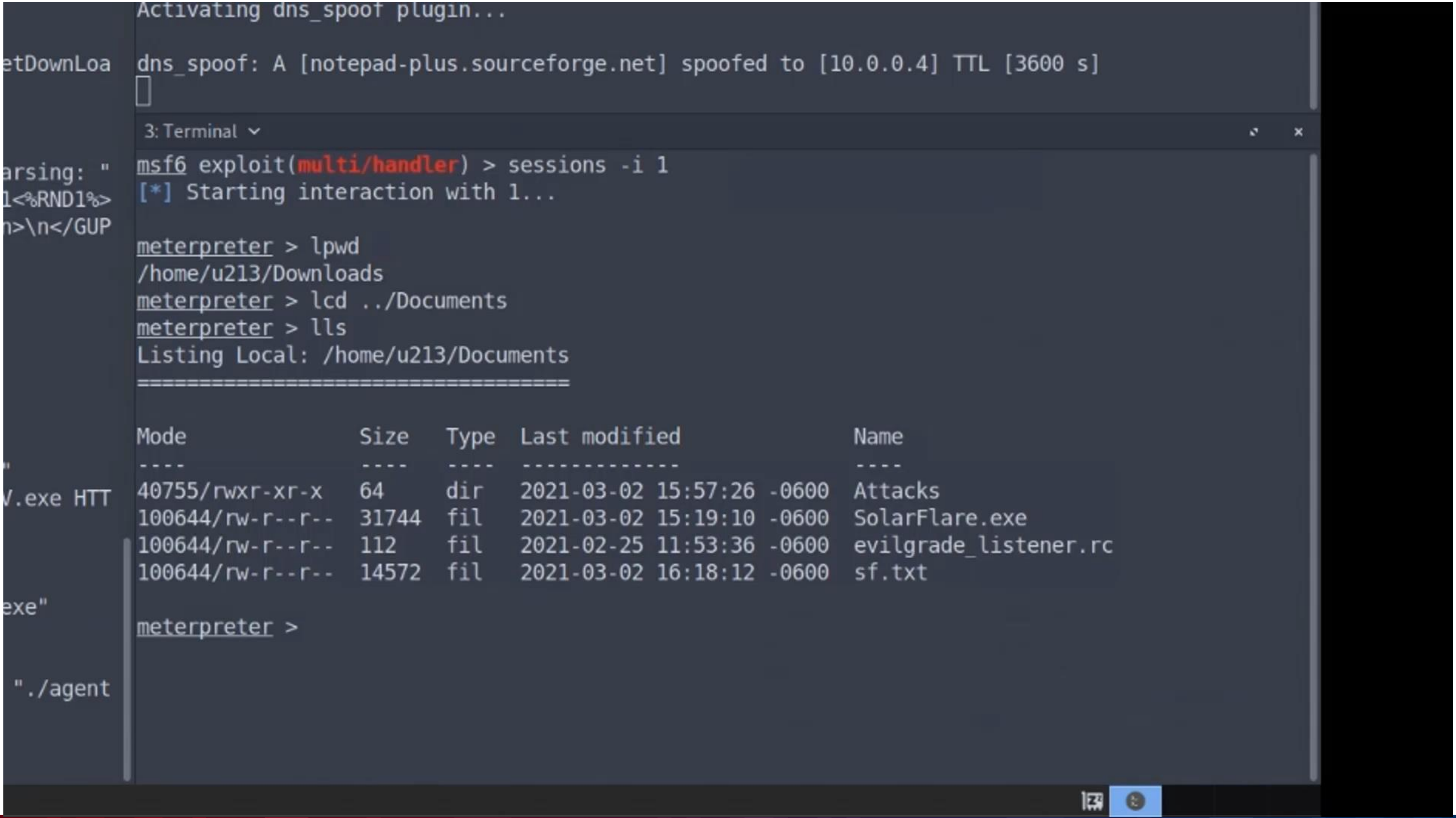


Staging the update

DEFENSE BREAKDOWN

- Endpoint protection to prevent the initial foothold.
- Credential Harvesting protection to protect the cred-store.
- Privilege Session Management to prevent lateral movement to Tier 0 assets.
- Privilege Threat Analytics to detect unauthorized behavior.

RECORDED DEFENSE DEMO



```
Activating dns_spoof plugin...

dns_spoof: A [notepad-plus.sourceforge.net] spoofed to [10.0.0.4] TTL [3600 s]
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > lpwd
/home/u213/Downloads
meterpreter > lcd ../Documents
meterpreter > lls
Listing Local: /home/u213/Documents
===================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40755/rwxr-xr-x   64     dir   2021-03-02 15:57:26 -0600  Attacks
100644/rw-r--r--  31744  fil   2021-03-02 15:19:10 -0600  SolarFlare.exe
100644/rw-r--r--  112    fil   2021-02-25 11:53:36 -0600  evilgrade_listener.rc
100644/rw-r--r--  14572  fil   2021-03-02 16:18:12 -0600  sf.txt

meterpreter >
```

ADULT FRIEND FINDER

CASE STUDY

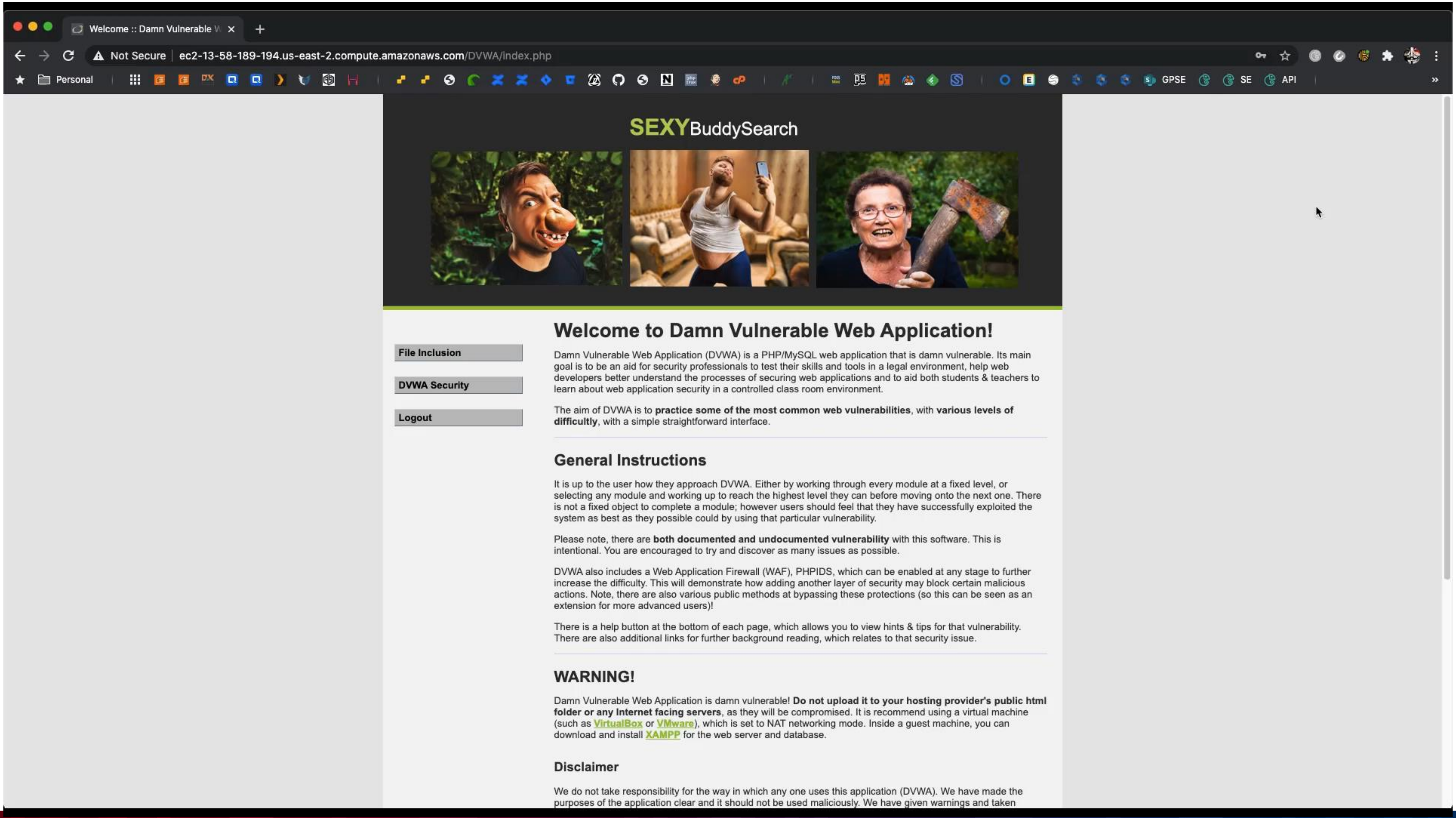
Adult Friend Finder

- October 18, 2016, “1x0123”, warned AFF Local File Inclusion (LFI) vulnerabilities on Twitter and posted screenshots as proof.
- 412 million user accounts have been exposed thanks to AdultFriendFinder Networks being hacked.
  - The breach included 20 years of historical customer data from six compromised databases:

ATTACK BREAKDOWN

- Path of the file is sent to a function which returns the content of the file as a string, or prints it on the current web page.
  - https://example.com/?download=brochure.pdf
- Path is changed to return an unintended file.
  - https://example.com/?download=../include/connection.php

RECORDED ATTACK DEMO



Welcome :: Damn Vulnerable W
Not Secure
ec2-13-58-189-194.us-east-2.compute.amazonaws.com/DVWA/index.php
Personal
GPSE
SE
API
SEXYBuddySearch
File Inclusion
DVWA Security
Logout

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

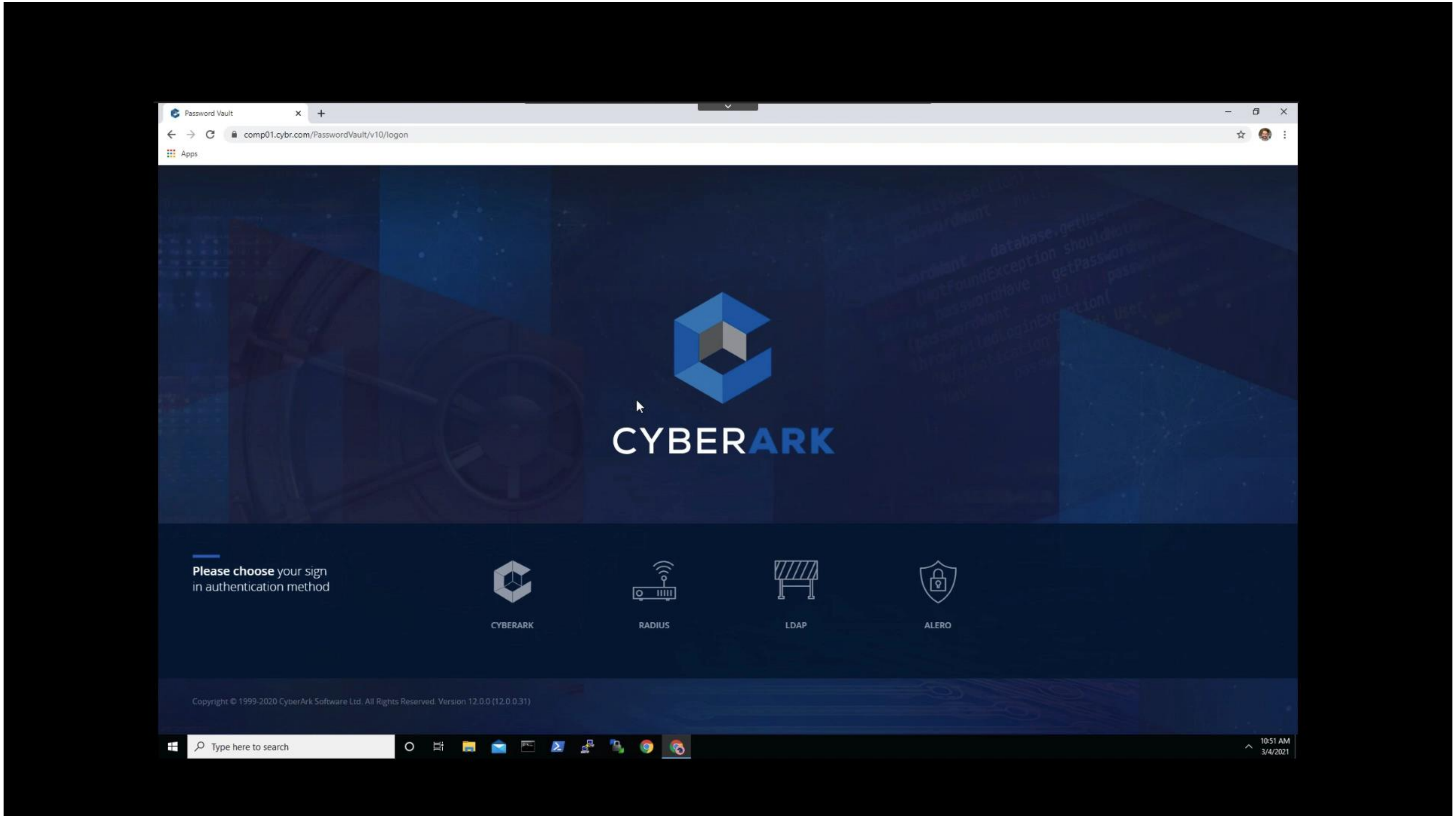
Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken

DEFENSE BREAKDOWN

- Little CYBR could do to prevent LFI.
- Save the file paths in a database and assign an ID to each of them. BY doing so users can only see the ID and are not able to view or change the path.
- Use a whitelist of files and ignore every other filename and path.
- Instead of including files on the web server, store their content in databases where possible.
- Protect credentials with STRONG password management.
  - Complex
  - Unique
  - Frequently Rotating

RECORDED DEFENSE DEMO



Please choose your sign in authentication method

Copyright © 1999-2020 CyberArk Software Ltd. All Rights Reserved. Version 12.0.0 (12.0.0.31)

OLDSMAR FLORIDA WATER TREATMENT FACILITY

CASE STUDY

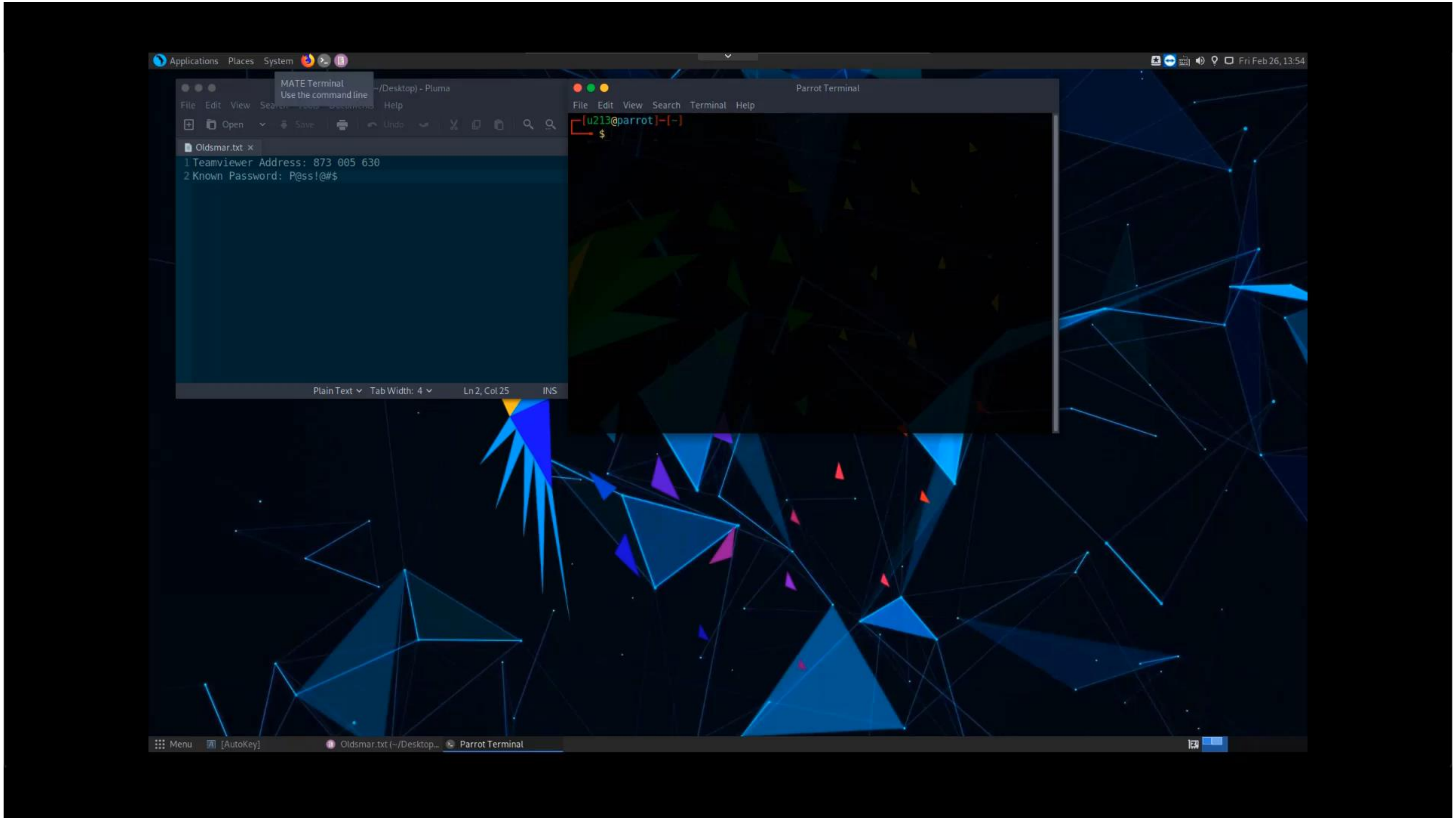
Oldsmar Florida

- First North American Hack where infrastructure was compromised.
- Feb 8th, 2021
- Accessed water treatment system remotely.
- Increased sodium hydroxide levels be a factor of more than 100x (FATAL).
- Plant operator quickly noticed the intrusion, reversed it, and no one was harmed.

ATTACK BREAKDOWN

- Running Windows 7
  (no longer supported and no security updates)
- Remote access tool TeamViewer.
  - Same password for all systems.
  - No longer used, but never uninstalled

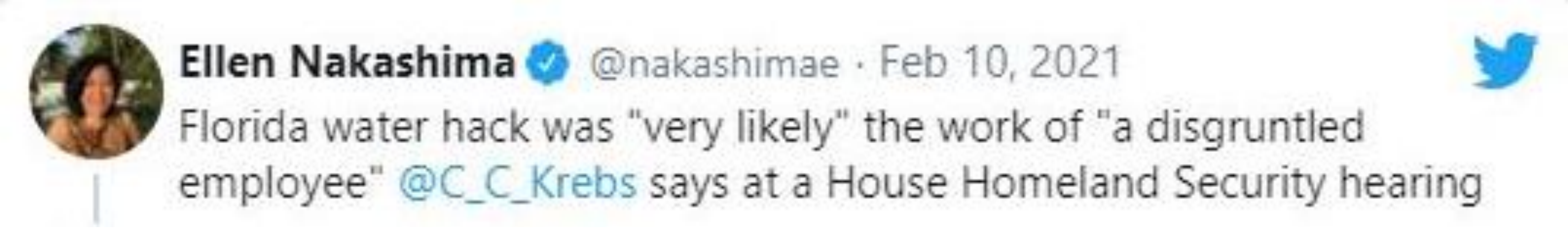
RECORDED ATTACK DEMO



```
Teamviewer Address: 873 005 630
Known Password: P@ss!@#$
```

```
┌─[u213@parrot]─[~]
└──╼ $
```

ATTRIBUTION



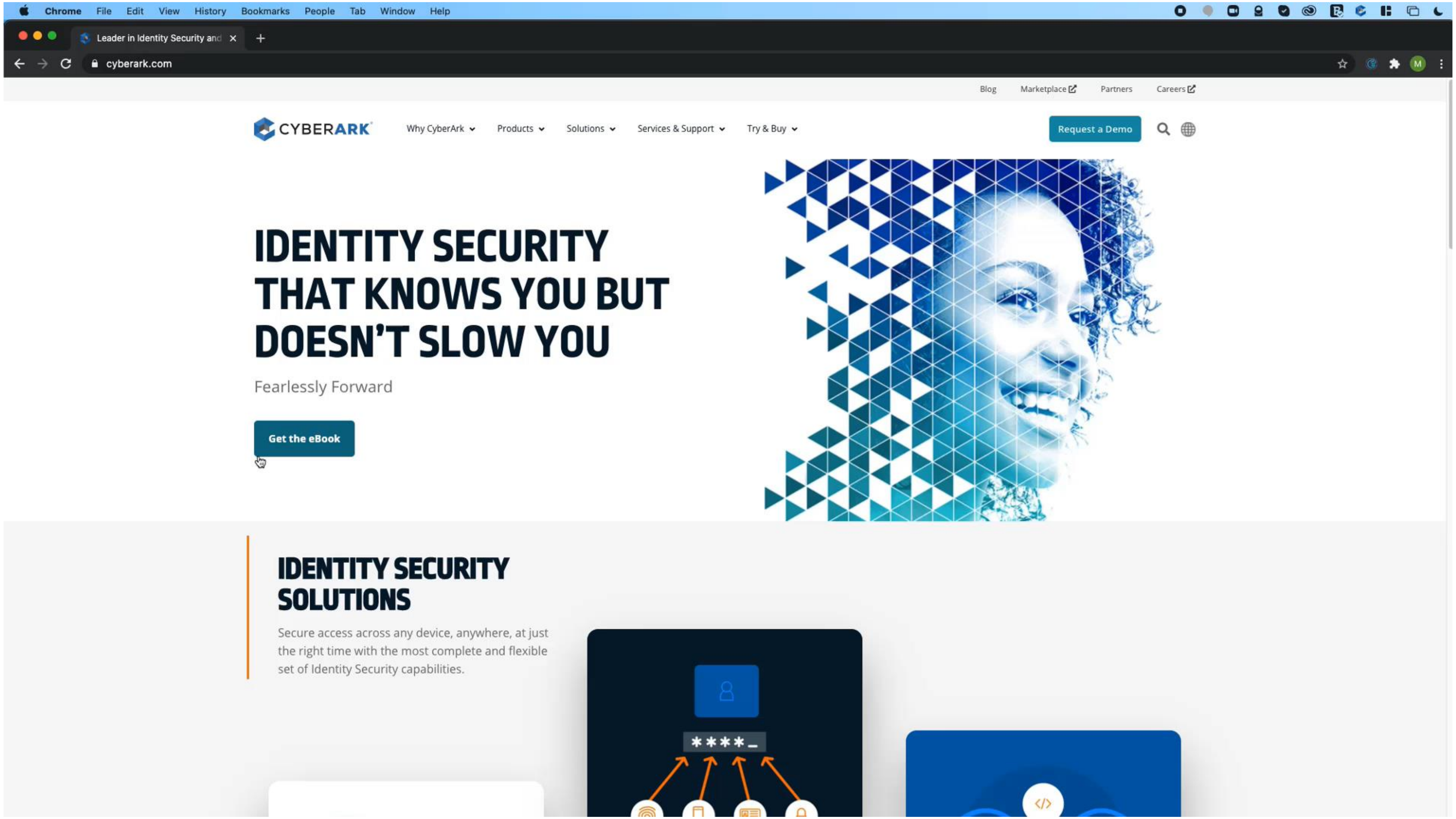
Ellen Nakashima @nakashimae · Feb 10, 2021

Florida water hack was "very likely" the work of "a disgruntled employee" @C_C_Krebs says at a House Homeland Security hearing

DEFENSE BREAKDOWN

- Disconnect ICS/SCADA systems from the internet.
- Run up to date and patched systems.
- Make passwords:
  - Unique
  - Complex
  - Frequently changing
- Use SECURE remote access software.

RECORDED DEFENSE DEMO



IDENTITY SECURITY THAT KNOWS YOU BUT DOESN'T SLOW YOU

Fearlessly Forward

IDENTITY SECURITY SOLUTIONS

Secure access across any device, anywhere, at just the right time with the most complete and flexible set of Identity Security capabilities.

CONCLUSION

CROSS PROMOTION SLIDES

QUESTIONS

SURVEY

CYBERARK

ATTACK & DEFEND

SERIES

THANK YOU