CYBERARK \ LABS

The Anatomy of the MGM Hack

A CyberArk Labs Perspective

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

Andy Thompson

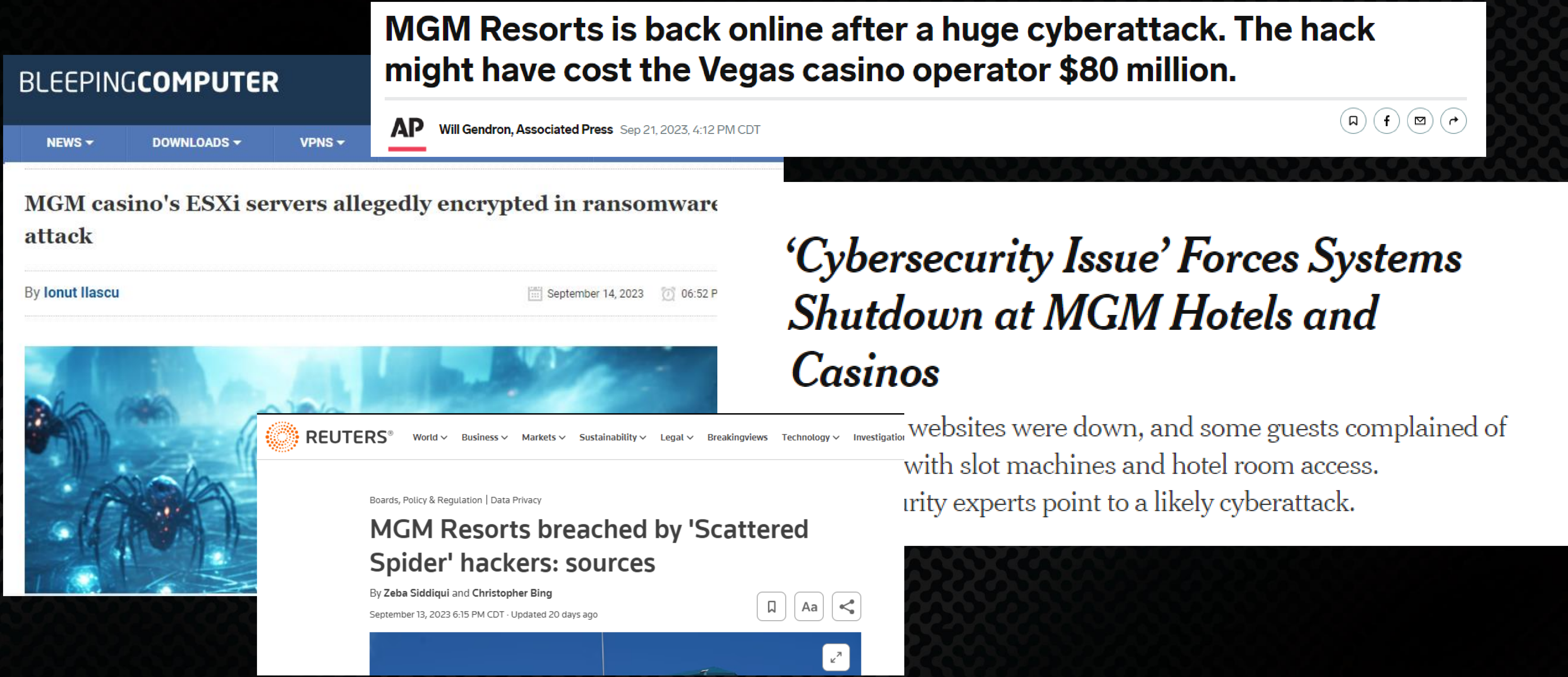
Offensive Security Research Evangelist

- SSCP/CISSP
- GPEN
- Emcee of Dallas Hackers Association
- Travel Hacker

in andythompsoninfosec

Andy_Thompson

Andy.Thompson@CyberArk.com



MGM Resorts is back online after a huge cyberattack. The hack might have cost the Vegas casino operator $80 million.

AP Will Gendron, Associated Press Sep 21, 2023, 4:12 PM CDT

BLEEPINGCOMPUTER

MGM casino's ESXi servers allegedly encrypted in ransomware attack

By Ionut Ilascu September 14, 2023 06:52 P

‘Cybersecurity Issue’ Forces Systems Shutdown at MGM Hotels and Casinos

websites were down, and some guests complained of with slot machines and hotel room access.

ırity experts point to a likely cyberattack.

REUTERS®

Boards, Policy & Regulation | Data Privacy

MGM Resorts breached by 'Scattered Spider' hackers: sources

By Zeba Siddiqui and Christopher Bing

September 13, 2023 6:15 PM CDT · Updated 20 days ago

MGM Resorts International

NYSE: MGM

- Hospitality & entertainment company.
  - Gaming, dining, entertainment, hotels & more.
- Headquartered in Las Vegas, Nevada.
  - Iconic resorts & casinos worldwide.

Scattered Spider

UNC3944, Scatter Swine, Muddled Libra, Storm-0875

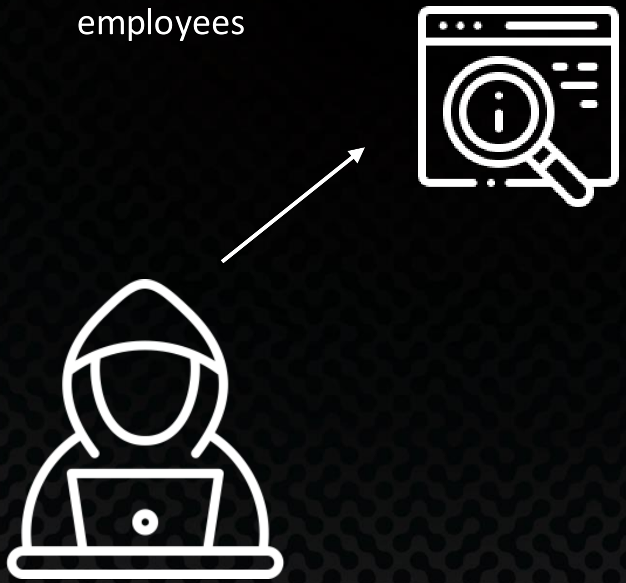
- Founded in May 2022.
- Common tactics:
  - SIM swap
  - Multi-factor bypass/fatigue
  - SMS/Telegram phishing
- Deep understanding of Azure, AWS, and GCP

AlphV/Blackcat

- Founded in 2020.
- Ransomware as a Service (RaaS) operator.
- Fast & thorough.

WhitePhoenix

MGM Attack Flow (September 2023)



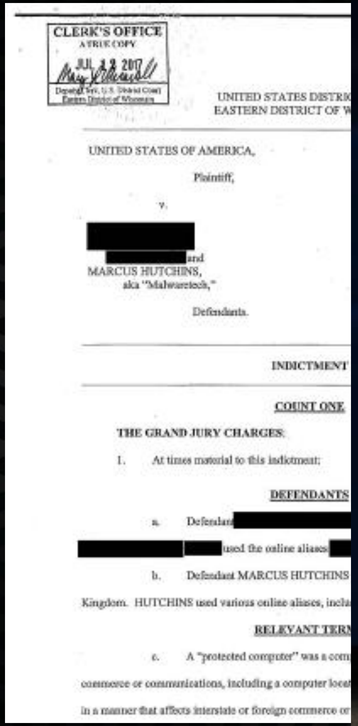
1. Gather intelligence about MGM and its employees

Open-Source Intelligence (OSINT)

- Publicly available information.
- Nothing new.
- OSINT is a tool.
- OSINT is a weapon.

Exhibit A: Dorks.

```
“Marcus Hutchins” filetype:pdf site:justice.gov
```



CLERK'S OFFICE
A TRUE COPY
JUL 12 2017
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRIC
EASTERN DISTRICT OF W

UNITED STATES OF AMERICA,

Plaintiff,

v.

[redacted]

[redacted]and
MARCUS HUTCHINS,
aka "Malwaretech,"

Defendants.

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES:

1. At times material to this indictment:

DEFENDANTS

a. Defendant[redacted]

[redacted][redacted]used the online aliases[redacted]

b. Defendant MARCUS HUTCHINS

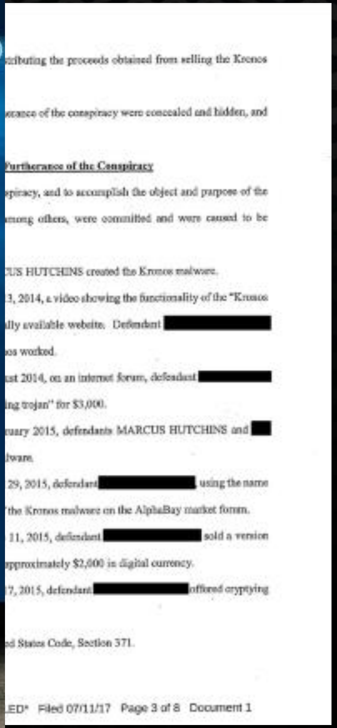
Kingdom. HUTCHINS used various online aliases, inclu

RELEVANT TERM

c. A "protected computer" was a com

commerce or communications, including a computer locat

in a manner that affects interstate or foreign commerce or



tributing the proceeds obtained from selling the Kronos

erance of the conspiracy were concealed and hidden, and

Furtherance of the Conspiracy

spiracy, and to accomplish the object and purpose of the

among others, were committed and were caused to be

CUS HUTCHINS created the Kronos malware.

13, 2014, a video showing the functionality of the "Kronos

ally available website. Defendant [redacted]

os worked.

ust 2014, on an internet forum, defendant [redacted]

ing trojan" for $3,000.

ruary 2015, defendants MARCUS HUTCHINS and [redacted]

lware.

29, 2015, defendant [redacted] using the name

the Kronos malware on the AlphaBay market forum.

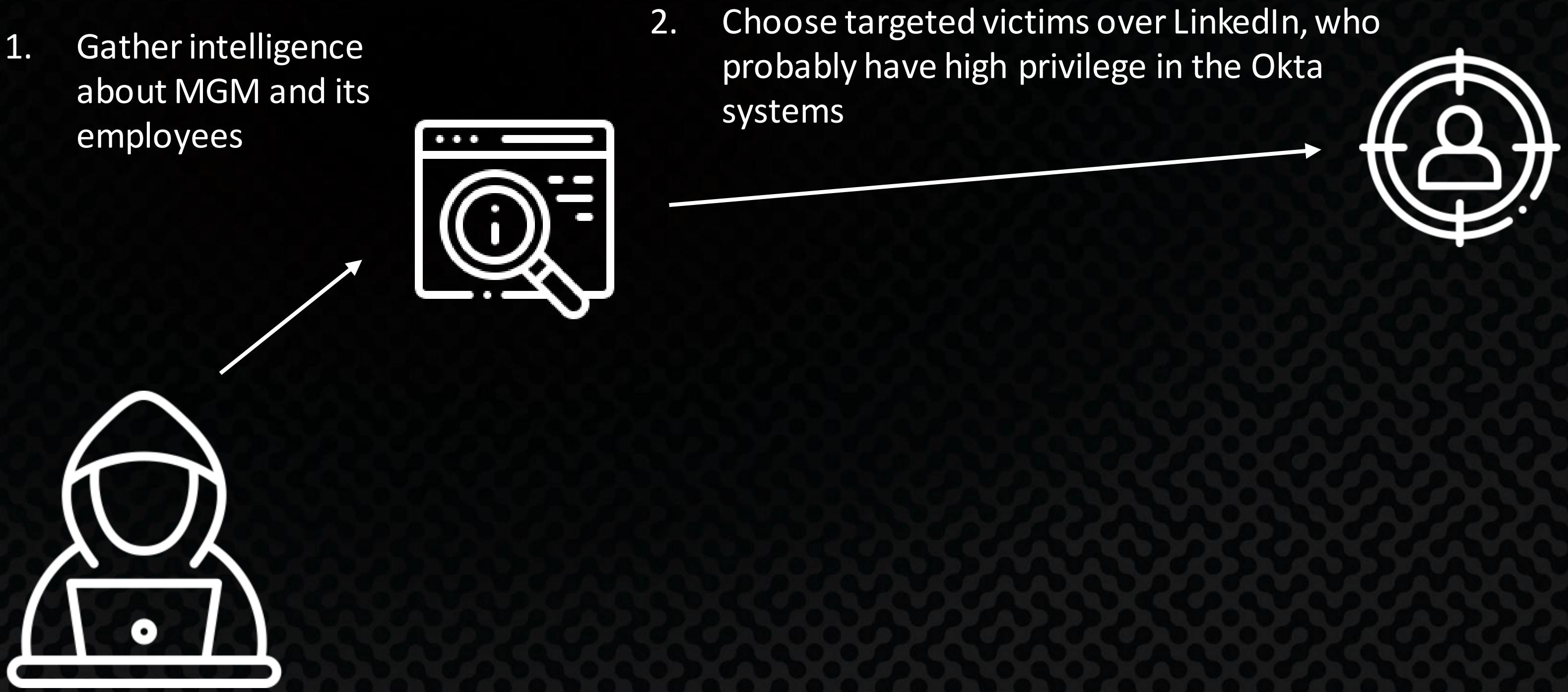
11, 2015, defendant [redacted] sold a version

approximately $2,000 in digital currency.

17, 2015, defendant [redacted] offered crypting

ed States Code, Section 371.

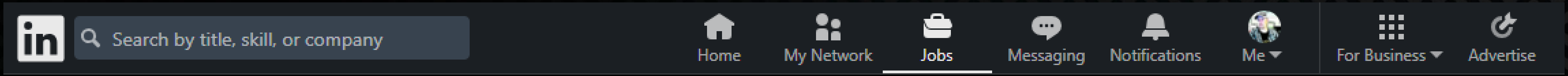
MGM Attack Flow (September 2023)

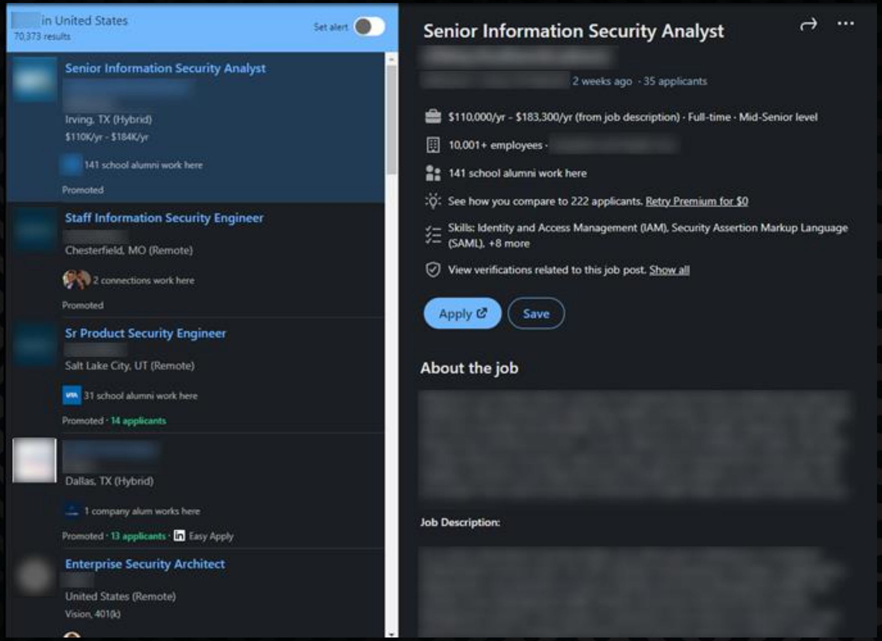


1. Gather intelligence about MGM and its employees

2. Choose targeted victims over LinkedIn, who probably have high privilege in the Okta systems

Exhibit B: Social Media




[redacted] in United States
70,373 results
Set alert

Senior Information Security Analyst
[redacted]
Irving, TX (Hybrid)
$110K/yr - $184K/yr
141 school alumni work here
Promoted

Staff Information Security Engineer
[redacted]
Chesterfield, MO (Remote)
2 connections work here
Promoted

Sr Product Security Engineer
[redacted]
Salt Lake City, UT (Remote)
31 school alumni work here
Promoted · 14 applicants

[redacted]
Dallas, TX (Hybrid)
1 company alum works here
Promoted · 13 applicants · Easy Apply

Enterprise Security Architect
[redacted]
United States (Remote)
Vision, 401(k)

Senior Information Security Analyst
[redacted]
[redacted] 2 weeks ago · 35 applicants

- $110,000/yr - $183,300/yr (from job description) · Full-time · Mid-Senior level
- 10,001+ employees · [redacted]
- 141 school alumni work here
- See how you compare to 222 applicants. Retry Premium for $0
- Skills: Identity and Access Management (IAM), Security Assertion Markup Language (SAML), +8 more
- View verifications related to this job post. Show all

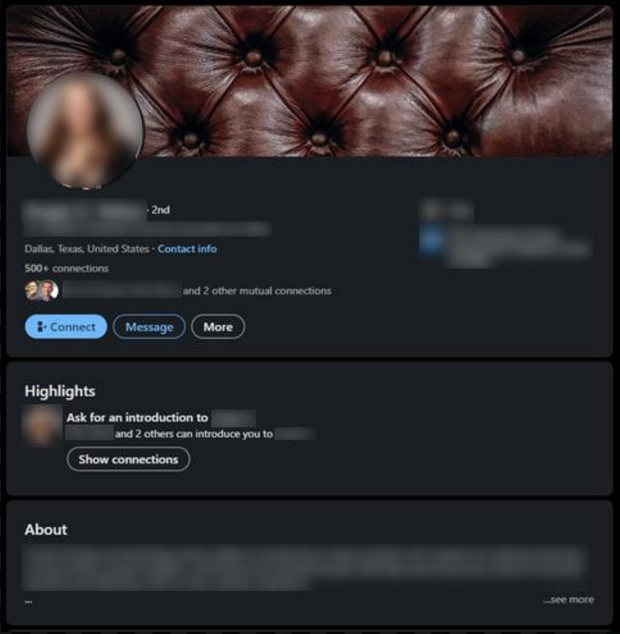
Apply Save

About the job

[redacted]

Job Description:

[redacted]


[redacted] · 2nd
[redacted]
Dallas, Texas, United States · Contact info
500+ connections
[redacted] and 2 other mutual connections

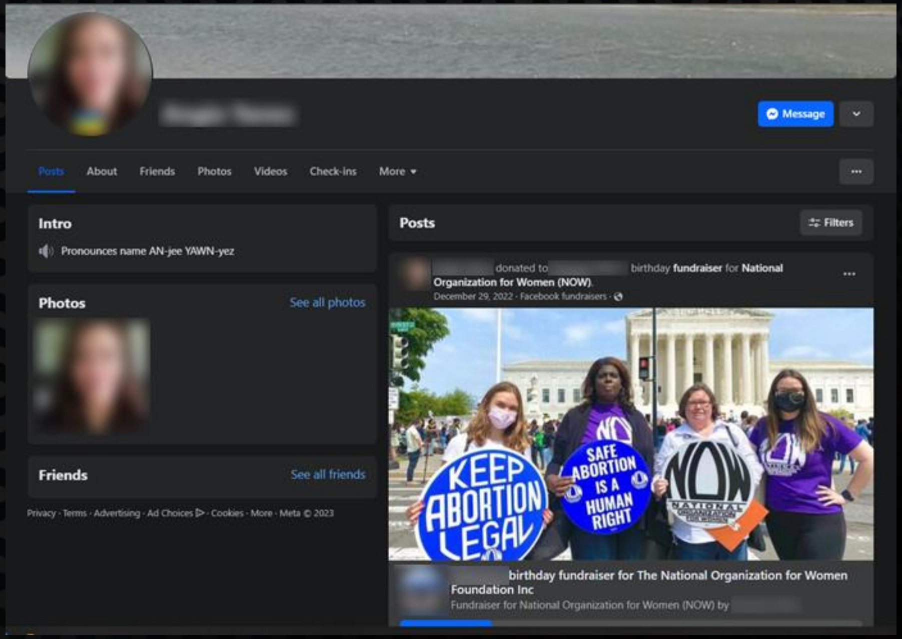
Connect Message More

Highlights

Ask for an introduction to [redacted]
[redacted] and 2 others can introduce you to [redacted]
Show connections

About

[redacted]
...
...see more


[redacted]
Message

Posts About Friends Photos Videos Check-ins More ▾

Intro
Pronounces name AN-jee YAWN-yez

Photos See all photos

Friends See all friends

Privacy · Terms · Advertising · Ad Choices ▷ · Cookies · More · Meta © 2023

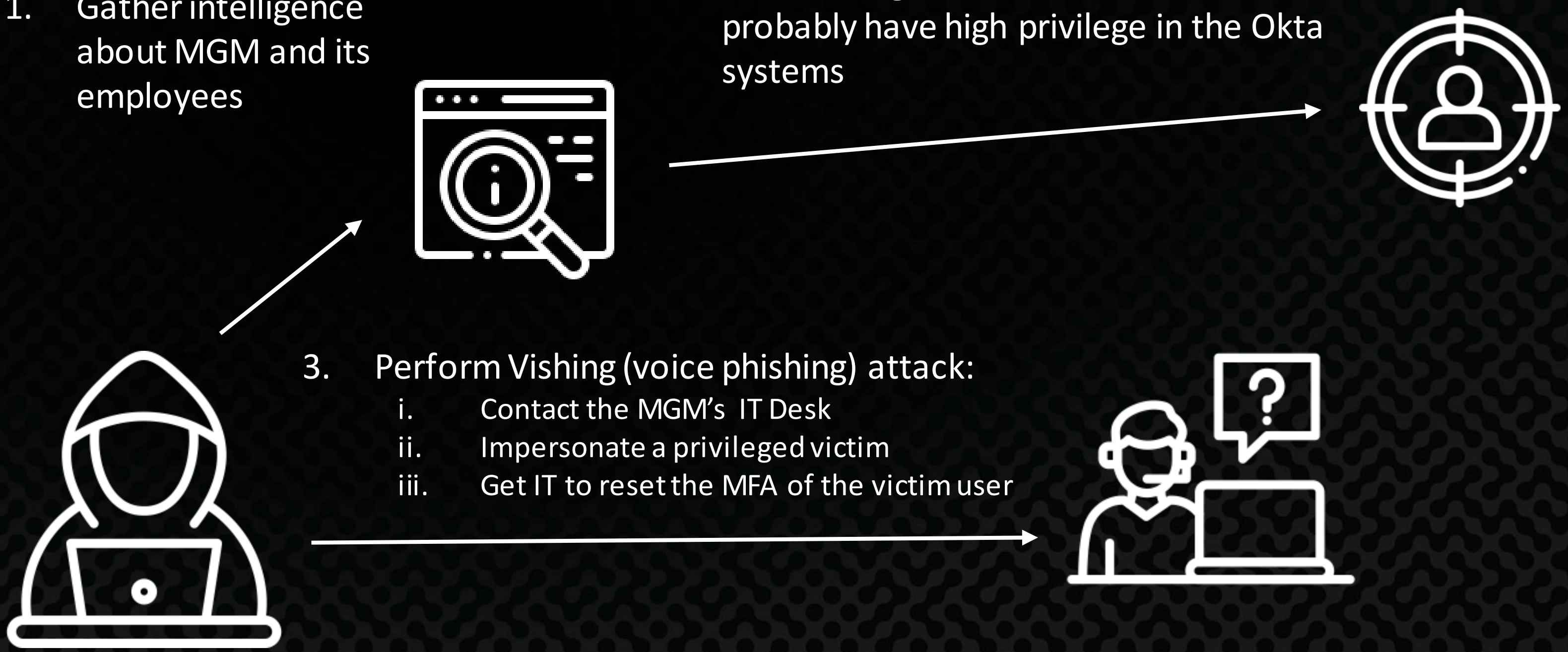
Posts Filters

[redacted] donated to [redacted] birthday fundraiser for National Organization for Women (NOW).
December 29, 2022 · Facebook fundraisers ·

KEEP ABORTION LEGAL
SAFE ABORTION IS A HUMAN RIGHT
NOW
NATIONAL ORGANIZATION FOR WOMEN

[redacted] birthday fundraiser for The National Organization for Women Foundation Inc
Fundraiser for National Organization for Women (NOW) by [redacted]

MGM Attack Flow (September 2023)



1. Gather intelligence about MGM and its employees

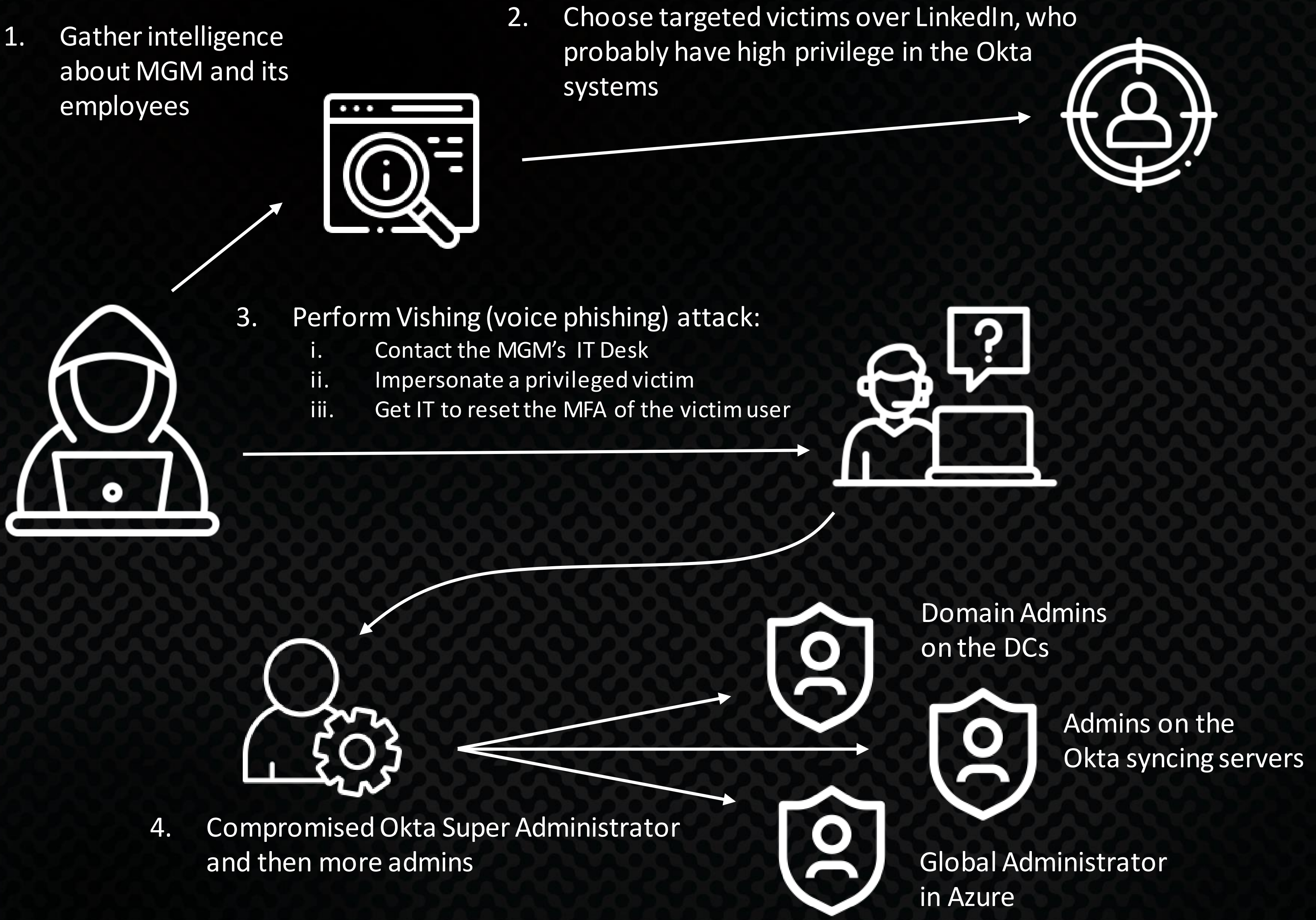
2. Choose targeted victims over LinkedIn, who probably have high privilege in the Okta systems

3. Perform Vishing (voice phishing) attack:
   i. Contact the MGM's IT Desk
   ii. Impersonate a privileged victim
   iii. Get IT to reset the MFA of the victim user

Social Engineering & Vishing

- Psychological manipulation.
- Vishing the helpdesk.
- Bypass MFA.
- Admin access to IAM.

MGM Attack Flow (September 2023)



1. Gather intelligence about MGM and its employees

2. Choose targeted victims over LinkedIn, who probably have high privilege in the Okta systems

3. Perform Vishing (voice phishing) attack:
   i. Contact the MGM's IT Desk
   ii. Impersonate a privileged victim
   iii. Get IT to reset the MFA of the victim user

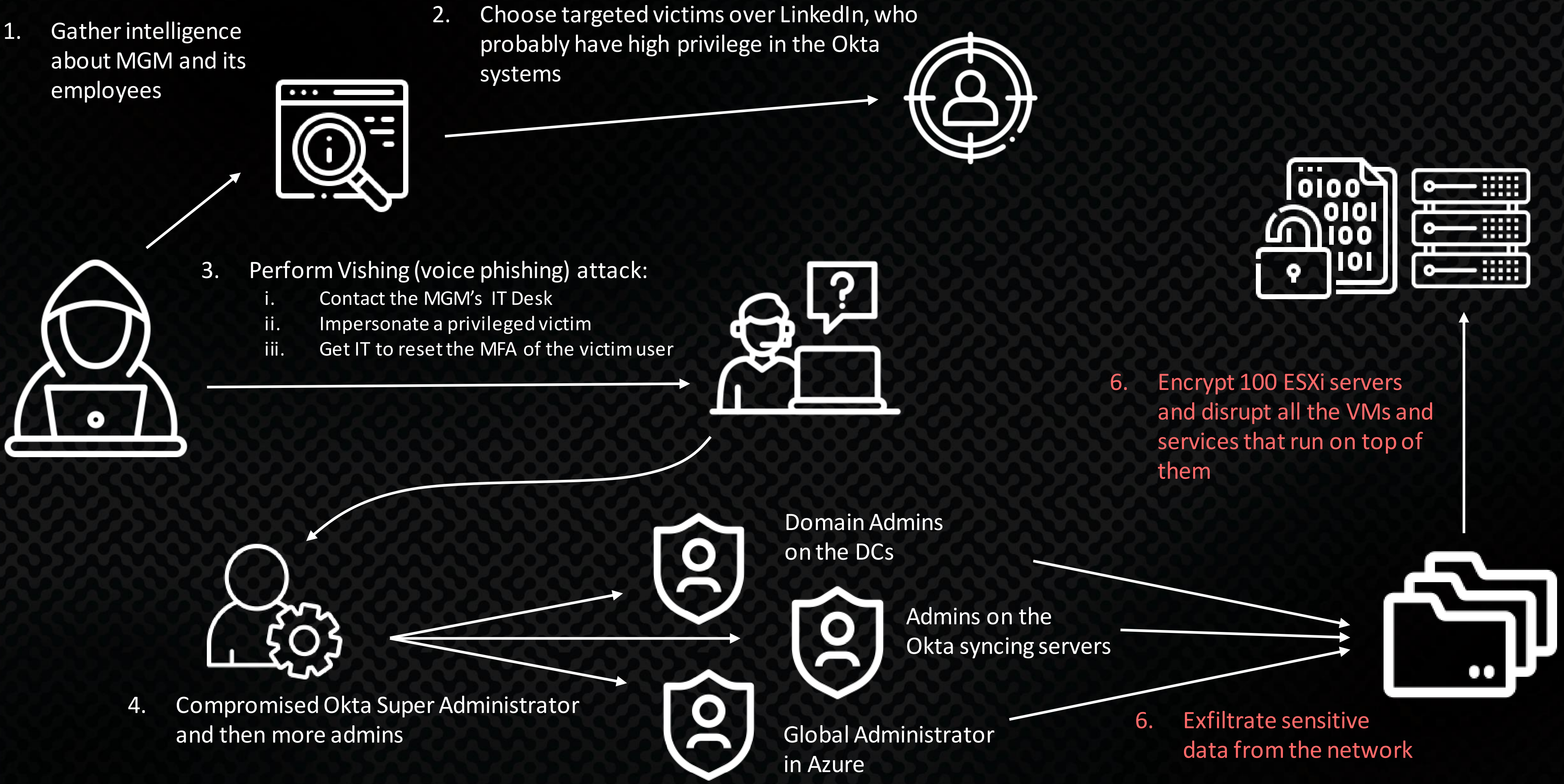
4. Compromised Okta Super Administrator and then more admins

Domain Admins on the DCs

Admins on the Okta syncing servers

Global Administrator in Azure

MGM Attack Flow (September 2023)



1. Gather intelligence about MGM and its employees

2. Choose targeted victims over LinkedIn, who probably have high privilege in the Okta systems

3. Perform Vishing (voice phishing) attack:
   i. Contact the MGM’s IT Desk
   ii. Impersonate a privileged victim
   iii. Get IT to reset the MFA of the victim user

4. Compromised Okta Super Administrator and then more admins

Domain Admins on the DCs

Admins on the Okta syncing servers

Global Administrator in Azure

6. Exfiltrate sensitive data from the network

6. Encrypt 100 ESXi servers and disrupt all the VMs and services that run on top of them

Security Failures

Potential Security Failures

- Password reuse & credential harvesting
- Social engineering.
- Limited visibility and control over privileged access.

Potential Security Failures

- Insecure configurations.
  - Credential syncing.
  - Inbound federation.
- Detection & response.

WE ARE CURRENTLY EXPERIENCING UNFORESEEN DIFFICULTIES, BUT ARE DILIGENTLY WORKING TO RESOLVE THIS AS SOON AS POSSIBLE. OUR SLOT MACHINES ARE AVAILABLE TO PLAY WITH CASH.

Effective security measures and best practices.

3 Critical Security Improvements

- Contain the impact
  - PAM & ZSP are vital starting points

- Increase MFA control points and scan for events
  - Establish dual control and stricter processes

- Endpoint security on all systems
  - Prevent the ransomware attack

IDP Best Practices

- MFA everywhere, especially on admin actions
- Enforce Helpdesk Verification methods
- Verify device enrollment and compliance
- Identify secure zones to reduce entry points
- Closely manage IDP Admin Accounts
- Monitor trust and admin changes

Thank you