AUTHENTICATION

Do You Know Who You're Dealing With?
How Authentication Affects Prevention, Detection, and Response

Who we are

Eric Scales | Mandiant

Director – IR, Red Team, Strategic Services

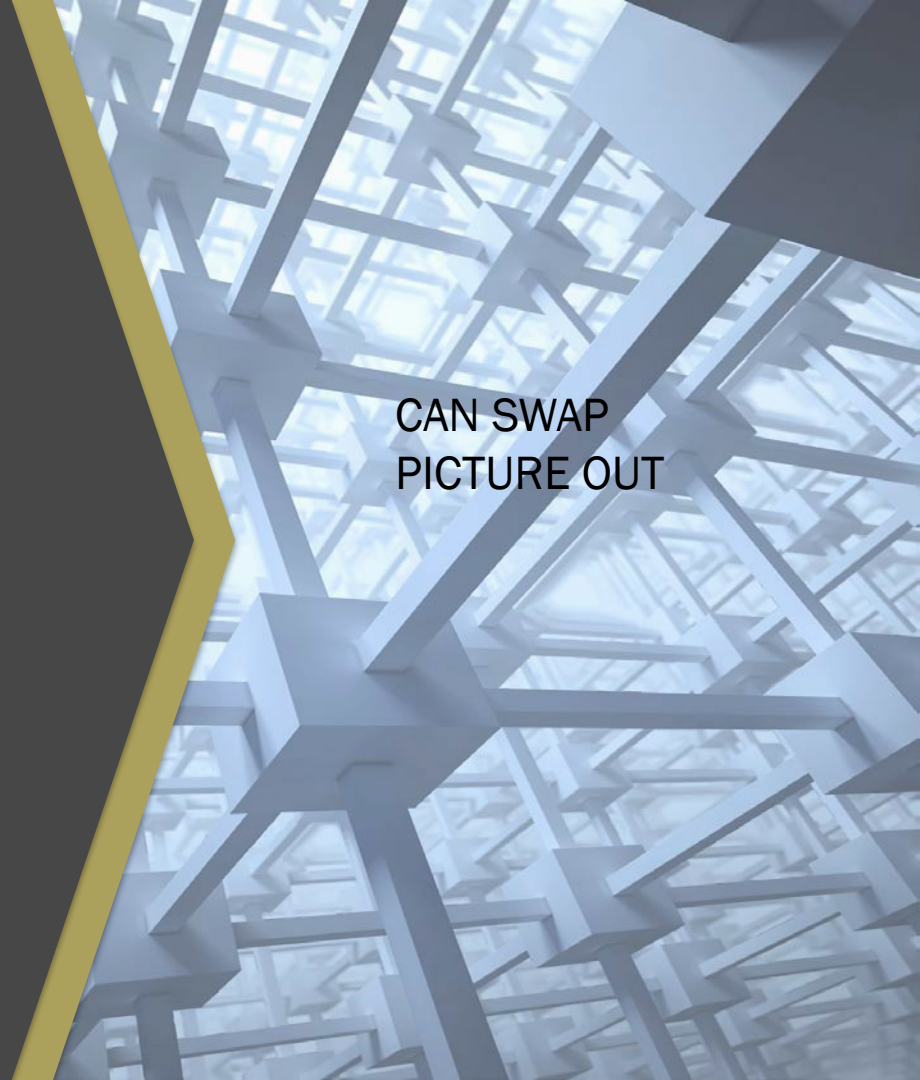
Scott Koller | BakerHostetler

Counsel, Privacy & Data Protection Team

Agenda

- The importance of authentication
- Detection
- Investigation and Response

The importance of authentication



Authentication

- Authentication is the act of validating an identity for the purposes of accessing <something>
- Used for tracking access to objects
- Authentication is a complex and sometimes misunderstood aspect of information security
- Significant issue with authentication is the trust placed by objects once authentication has taken place

Core authentication types

- Single factor authentication
  - Passwords
  - Biometrics
- Multi-factor authentication
  - Something you know + something you are/have
- Single Sign On (SSO)
  - OAUTH
  - Cookies

Authentication

- Is critical in proving/disproving legitimate vs. malicious activity
- Malicious insider vs. remote attacker
- Unwitting insider vs. malicious insider vs. remote attacker

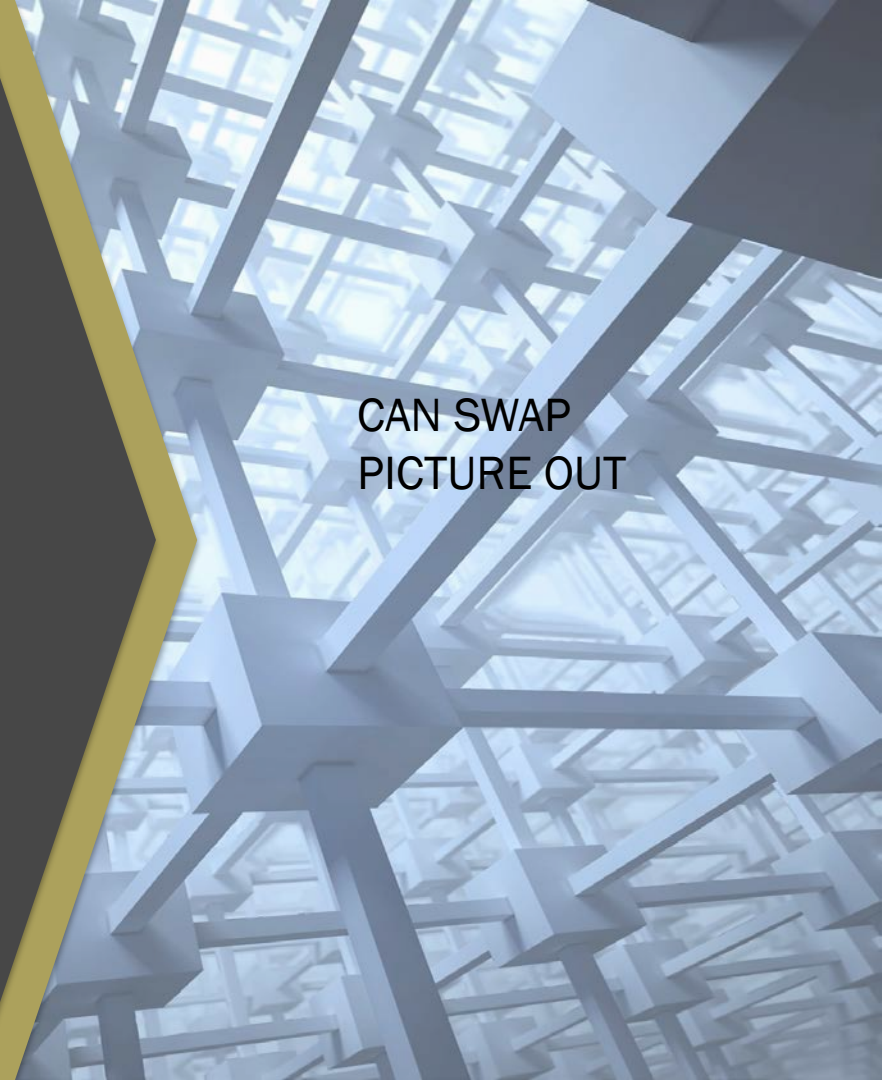
Example – auth criticality

- Hacked bank
  - Attacker transferred large sums of money to multiple bank accounts
  - Money transferred to “other parties”
  - Money laundered through various business enterprises
- Was an insider involved?
- How do you prove the answer to this question?

The Legal challenges

- Notification laws are triggered by unauthorized access to certain data
  - Uncertainty – err on the side of caution?
  - Worst case scenario
- Data outside coverage of notification laws
- Pursuing recovery of losses
- Other consequences

Detection



Detection time

146
DAYS

Median days for compromise to discovery

External Notification	Internal Discovery
320 days	56 days

3 days

Average number of days for Mandiant red team to gain domain administrator credentials

Need to think about security from the perspective of an attacker, not as a defender

NASCUS

Detection time

47% INTERNATIONAL DISCOVERY OF BREACH

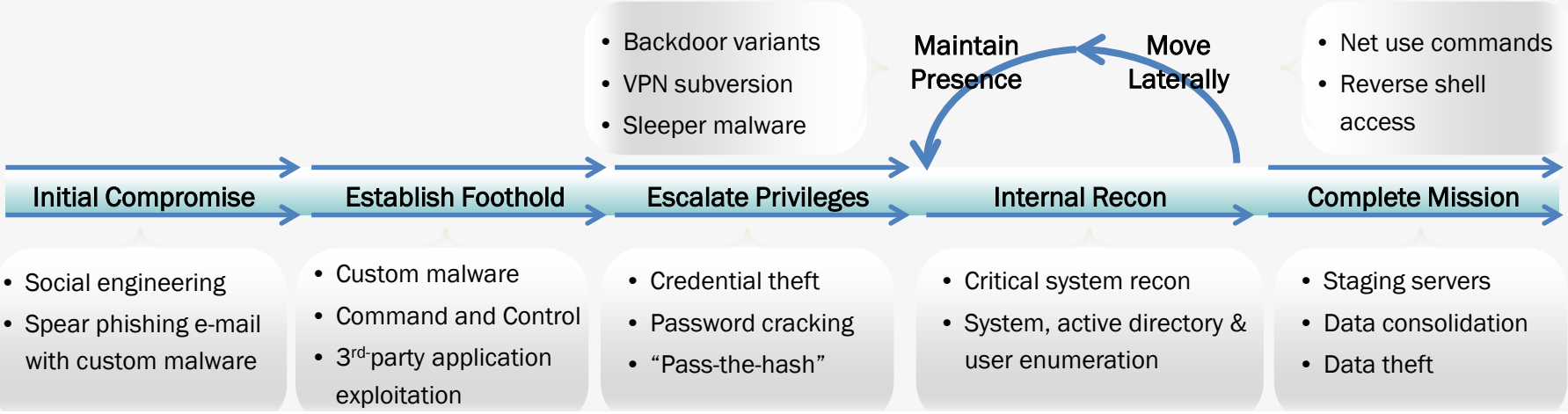
53% EXTERNAL NOTIFICATION OF BREACH

NASCUS

Fundamental truths

- Breaches are inevitable but they can be mitigated
- The goal of any cyber security program: *to eliminate the consequences of a cyber security breach, not necessarily the breach itself*
- Every breach relies on authentication at some point in time
  - Focusing on authentication is essential to detecting and responding to every breach

Are you prepared?



	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Recon	Move Laterally	Maintain presence	Complete Mission
Prevent	✔					✔	
Detect	✔		✔				
Respond					✔		

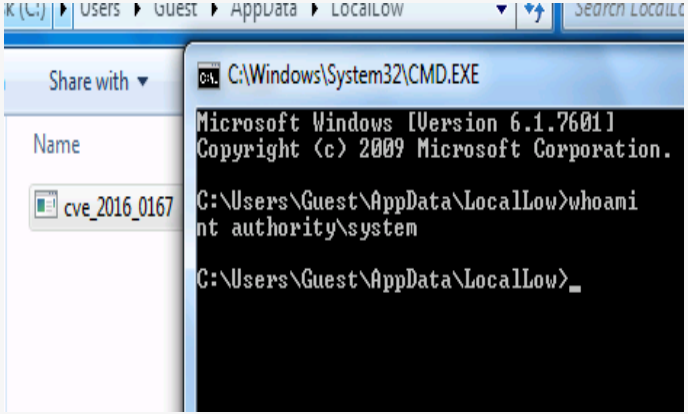
Credential theft

- How do they get those credentials external to your network?
  - Spear phishing
  - Watering hole attack (strategic web compromise)
  - Exposed through major breach
  - Password re-use

LinkedIn Lost 167 Million Account Credentials in Data Breach

Privilege escalation

- How do they get those credentials inside your network?
  - Zero-day exploits
  - Pass-the-hash (Mimikatz/WCE)
  - Golden/silver ticket attack
  - Vulnerable services running as admin
  - File shares
  - Code



Detecting credential misuse

- Understand all places where user authentication occurs
- Understand how authentication works in your environment
- All authentication logs must be sent to single location
- Perform correlation and time correction

Detecting credential misuse

- Create and tune rules for your organization
  - Use geolocation
  - Use machine learning/baselining
- Send email summarizing all activity to administrative users
- Ensure alerts are investigated thoroughly – all malicious activity will leverage user credentials at some point

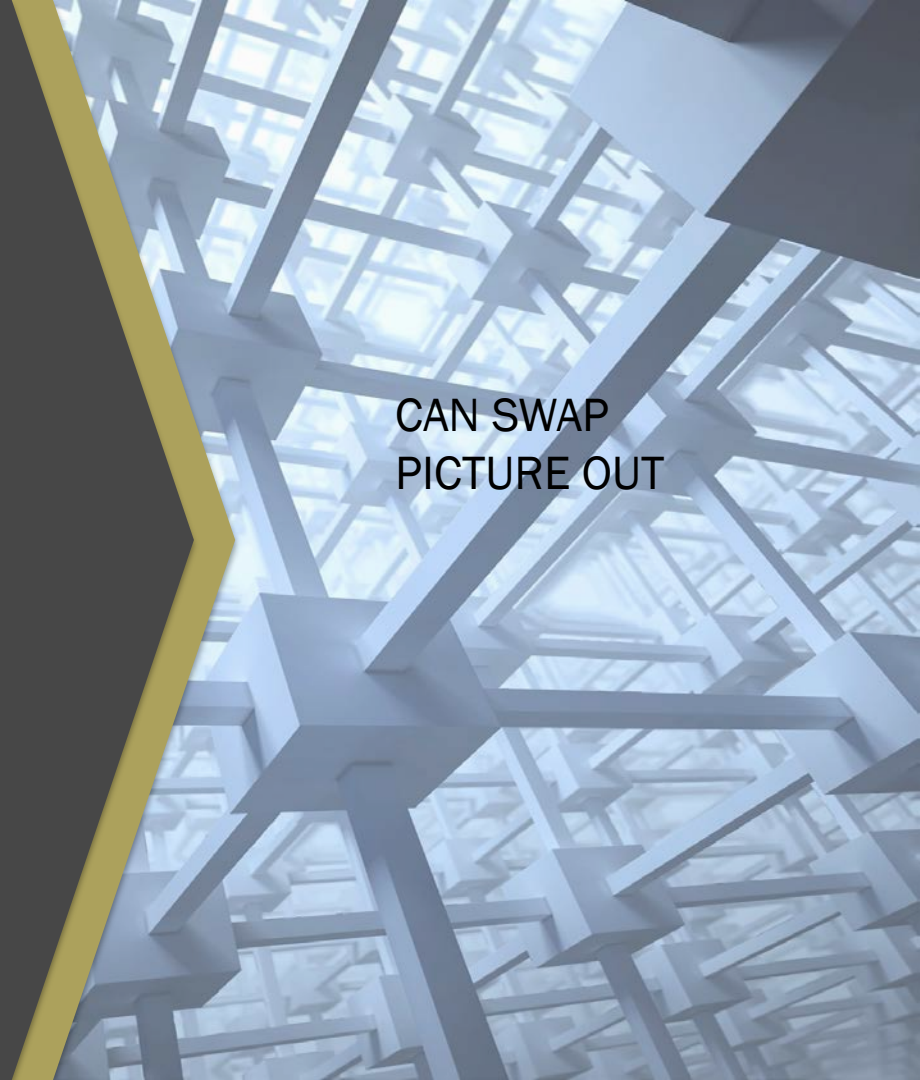
Use Case

- Client used two-factor authentication (password + token) to validate users on VPN
- Attacker modified server settings to create a temporary token (often used in conjunction with lost tokens)
- Attacker leveraged temporary token in conjunction with stolen credentials to authenticate to VPN as legitimate user
- MFA server stored configuration change information in a local log file – evidence was there but no one was looking

Use Case – what was missed

- Temporary token issued to user
- User authentication to VPN from <evil country>
- User authentication to VPN in anomalous fashion
- User that authenticated to VPN should not have been able to use Domain Administrator account after authenticating
- Domain Administrator account operating in anomalous fashion

Investigation & Response



Incident Response Timeline

69 DAYS
Occurrence to discovery

7 DAYS
Discovery to containment

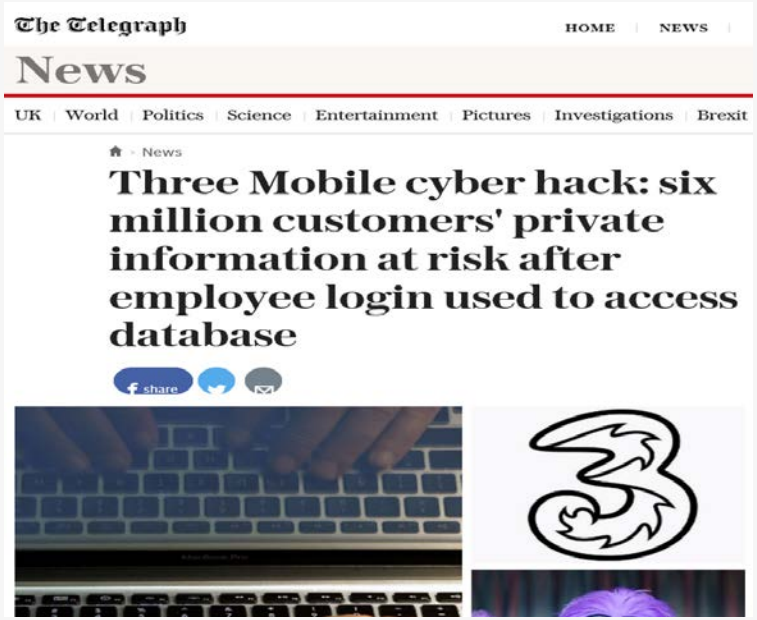
43 DAYS
Engagement of forensics until forensic investigation complete

40 DAYS
Discovery to notification

BakerHostetler Data Security Incident Response Report 2016

Examples – external single factor

- VPN/OWA
- Cloud services (e.g., Outlook 365)
- Vendor portals (e.g., payroll, W2s)



Examples – external single factor

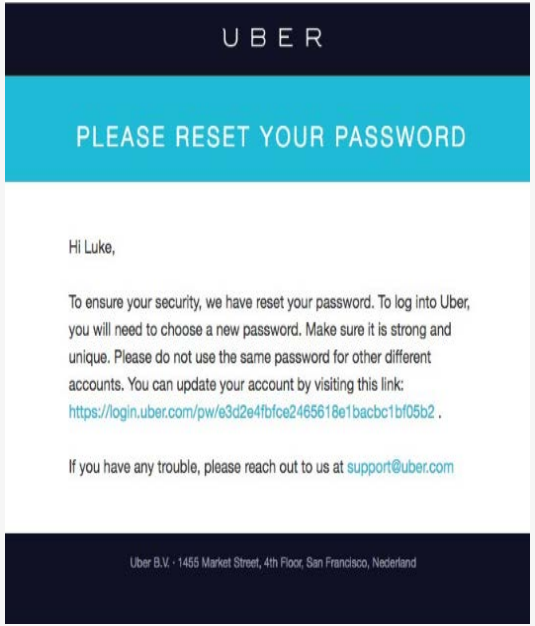
- SSO (OAUTH 2.0 common)
  - Third party malicious app intercepts traffic
  - Attacker authenticates to application
  - Attacker substitutes username w/ victim username
  - Authentication successfully bypassed

Scenarios – Internal single factor

- Admin access to segmented environments with sensitive data (e.g. cardholder data environment)
- Access to accounts that permit theft of funds
- Financial reporting systems – reliance on internal controls?

Scenarios – Account takeovers

- How were the credentials obtained?
- Whack-a-mole defense?
- Proactive notice?
- Impact
  - Customer experience
  - Alter reward/account value
  - Resources
  - Fraud losses



Questions