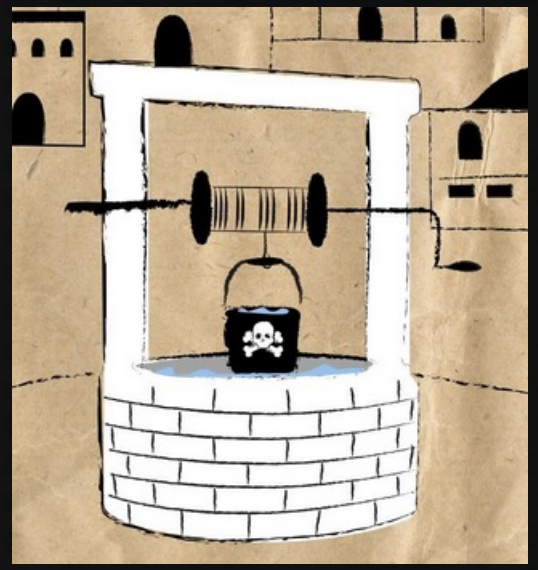
Attack Tactics #8
Poisoning the Well

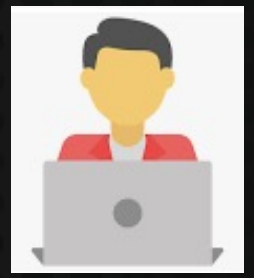


Attack Overview

Spray

Office

Push



Auth

SharePoint

OneDrive

Poison

Sync

BLACK HILLS
Information Security
2008

Core Issues

- User Awareness to Social Engineering (Unsolicited Push)
- Azure Active Directory Exposed to Users
- Macro-Enabled Documents on SharePoint
- Documents Potentially Replicated To/From File Shares

@BHInfoSecurity

Benefits

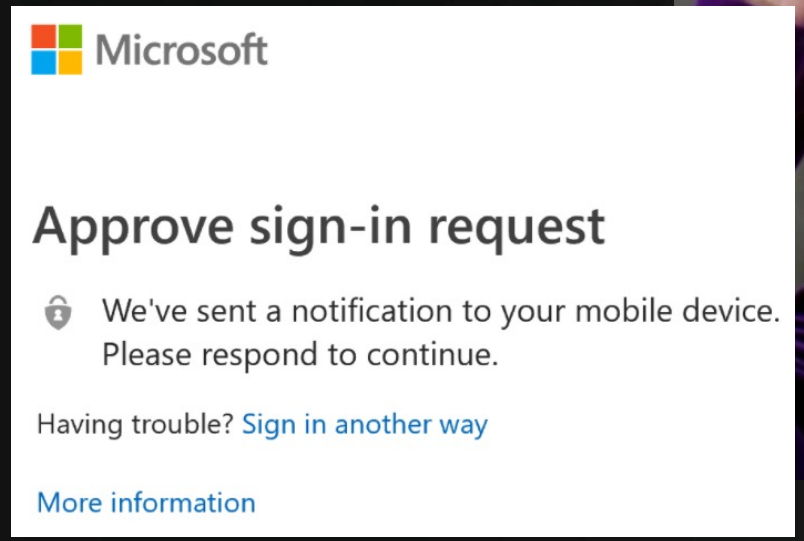
- No Need to Bypass Phishing Controls
  - Spam Filtering
  - Attachment Filtering
  - Categorization Filtering
  - Execution Prevention
  - User Reporting
- Documents ALREADY Trusted
- Difficult to Trace

The Breakdown – Step 1

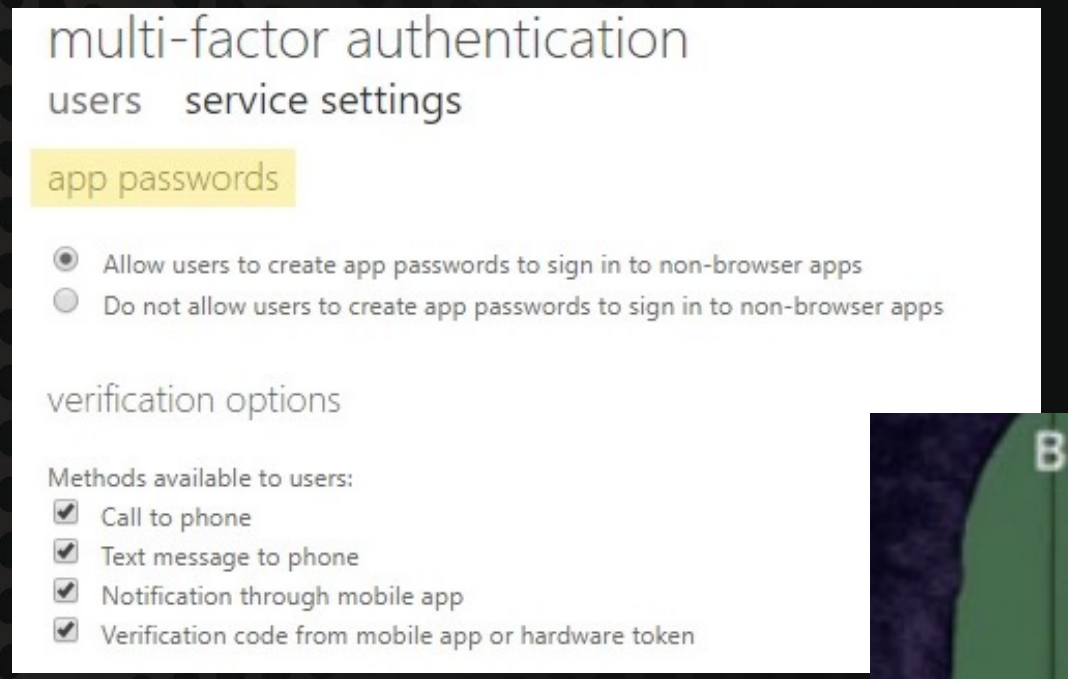
- Gather Employee Information for Password Spraying
  - Scrape LinkedIn User Details from LinkedIn
  - Public Breach Dumps
- Password Spray Office 365 for Initial Access
  - Graph API Indicates Auth Success when MFA is Enabled
  - SmartLockout Thwarts Direct Attacks
  - Attacks via Proxy Services Highly Effective
    - FireProx – AWS Lambda Solution
    - Proxycannon-ng – OpenVPN Solution

The Breakdown – Step 2

- Send Unsolicited Push Notifications to Users
  - User Can Respond without Thinking
  - Timing is Important – Hit When Expected
    - Beginning of Work Day
    - After Typical Lunch Hour
  - Other MFA Options May Also Work



The Breakdown – Step 3



- Configure and Use Backup MFA
  - App Password
  - Alternate Phone
  - Device Code Access

The Breakdown – Step 4

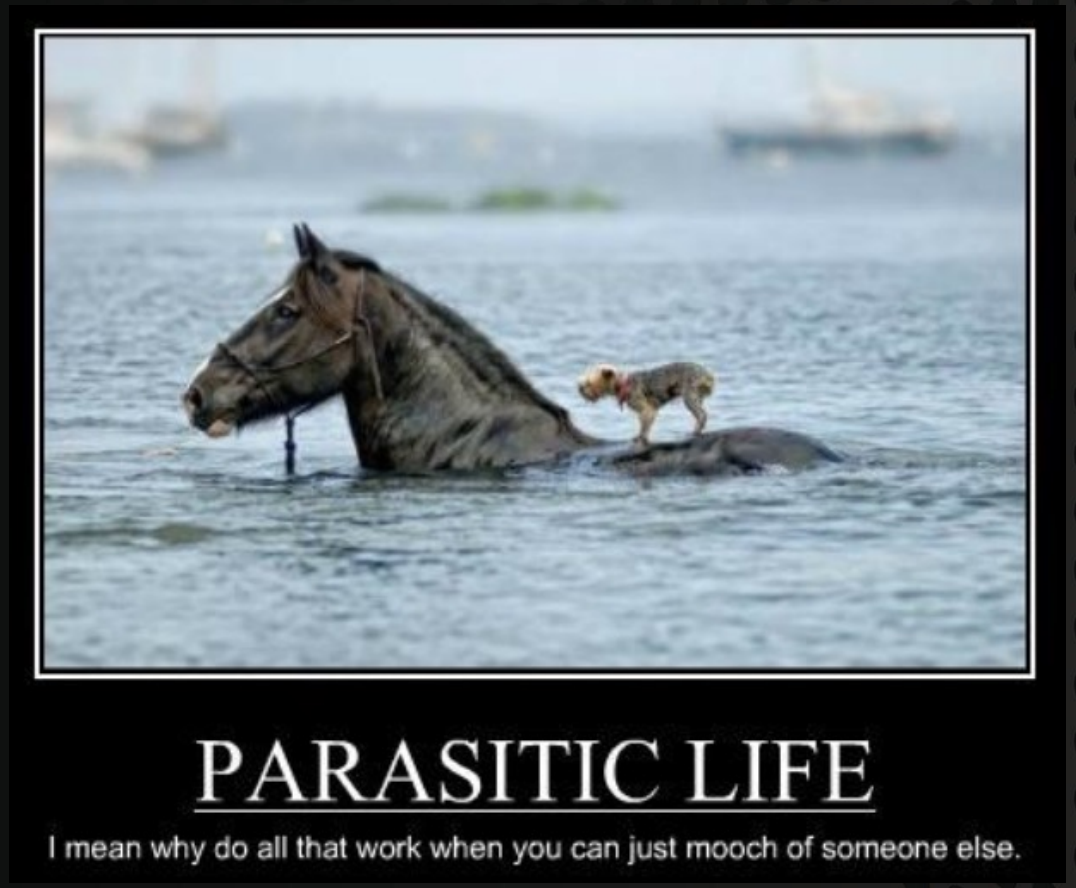
- Check for Azure AD Portal Access
  - Accessible by Default
  - Cloud Version of Active Directory Users and Computers (ADUC)
  - May Contain Sensitive Information
  - Offline Backup Possible
  - Improves Other Attacks (Like Password Spraying)

The Breakdown – Step 5

- Check for OneDrive/SharePoint Content
  - Search for Implantable File Types
    - Macro Enabled Documents (.docm, .xlsm, .pptm, etc)
    - Development Artifacts (.proj, .csproj, etc)
    - Scripts (.bat, .ps1, .vba, etc)
  - Check Access/Modify Dates
  - Check for Concurrent User Access

The Breakdown – Step 6

- Poison the Well
  - Generate Malicious Content for Targeted File Type
  - Download Target File
    - Test Implant Method and Execution
    - Ensure Functionality is Not Disrupted
  - Embed Tested Payload Into Target File
  - Also works well for lateral movement
  - Profit $$$$$



Payload Considerations

- LOLBin Execution
- Direct Persistence
  - Registry keys
  - Startup Folder
- Payload Doesn’t Have to be Overtly Malicious
  - Host Reconnaissance
  - Active Directory Reconnaissance

Attack Tracing Difficulties

- Executed by Authorized Individual
- No Message, Subject Line, or URL to Correlate
- Active Documents are EDITED by Users
  - Difficult to Identify Initial Infection User w/o Version History
  - Difficult to Identify Origin of Malicious Content

@BHInfoSecurity

Recommendations

- Educate Users on MFA Indicators of Compromise
  - Unsolicited Push, Phone Call, SMS
- Change Passwords on Affected Accounts
- Check for Backdoor Account Access
  - Alternate MFA Options
  - App Passwords
  - Device Code Access
- Restrict Access to Azure AD Portal

@BHInfoSecurity

Follow-Up

- Next attack tactics webcast:
  - Instrumented deployment analysis
  - Identify opportunities for detection/prevention
  - Develop supporting optics
  - Detailed SOC detections!
    - Baseline endpoint controls include Defender and Sysmon
    - WEC / WEF setup forwarded to Elastic

@BHInfoSecurity

Questions?

@BHInfoSecurity