Two Factor Evolution:
How Attackers Evade Multi-factor Authentication and What Organizations Can Do About It
Roadmap

- Introduction
- MFA – A Luxury You Can’t Afford to Skip
- MFA In Practice – Operational Needs vs. Security Posture
- A New Threat Model for MFA
- How Attackers Approach MFA
- How Your Teams Should Approach Defending It
  - (If They Aren’t Already)
- Conclusion
Introduction

Your intrepid explorers of all things multi-factor

- Austin Baker
- Principal Consultant – 5 years with Mandiant/FireEye
- Blue Team Turned Red Team
  - Turned... purple?
- Long-time DM and cat owner
Introduction

Your intrepid explorers of all things multi-factor

- Doug Bienstock
- Senior Consultant – 4 years with Mandiant/FireEye
- Incident Response and Red Team leader
- Lifelong Green Bay Packers fan
The Obvious – You Need MFA

- For Internet-facing services with sensitive data – no longer optional
- Still not universally adopted
- Root cause of many day-to-day security headaches
  - Business email compromise
  - Direct deposit fraud
  - User impersonation fraud

- “We have it, so we’re all good then, right?”
  - Well…
The Obvious – But What Is MFA

- Canonical definition is still the best
- Choose at least 2 of:
  - Something you have (token, phone, etc.)
  - Something you know (password, secret question, PIN, etc.)
  - Something you are (fingerprint, biometric measure, etc.)
- Limitation you can’t (and shouldn’t) try to get around
MFA: Necessary, But Not Sufficient

- The era of “set-and-forget” MFA is over (because it never really started)
- Operational needs compromise security best-practices
  - Exceptions
  - Administrator management
  - Help Desk integration
- Deploying effective MFA solution can be complex
- What was once seen as unassailable…
  - … is now part of many advanced attacker methodologies
An Evolving Multi-factor Landscape

How changing trends effect attacker priorities

- Started researching effective bypasses in 2015
  - Physical tokens common
  - Software and phone token usage growing
- Now, software-based tokens are for at-scale:
  - SSO
  - External web mail
  - VPN access
  - Critical internal systems
- As MFA power increased, so did attacker interest
A Novel Approach – MFA Threat Model

Creating an MFA-specific security model

Motivations:
- MFA is a unique, but integral part of a strong security posture
- Effective attacks are implementation specific
- As are effective defense strategies

Solution:
- Isolate the stages of attacker activity aimed at MFA
- Define common techniques to bypass or backdoor it
- Build strategies for defenders to address each stage
MFA Threat Model
A simple framework for modeling MFA attacks

**Pre-Authentication**
- Before the user logs in – how attackers capture MFA sessions

**Post-Authentication**
- How attackers maintain access within the MFA system

**Post-Exploitation**
- Turning a compromised Domain Admin into permanent MFA access
Pre-Authentication
How attackers get their foot in the door
Pre-Authentication: The Setup

- What Attackers Have:
  - Target organization and MFA product identified
  - Targeted users
  - User credentials (probably)
  - Objective
  - Effective, asymmetrical social engineering techniques

- What Attackers Need:
  - A way to turn phishing into MFA access
Pre-Authentication: Casing the Joint

- Identifying scheme in use is often easy
  - LinkedIn results or job postings
  - Testing stolen credentials
- What attackers look for:
  - Target MFA product
  - Source of second-factor
    - (phone, physical, software token)
  - Delivery mechanisms that are supported
    - SMS/Phone call
    - Push
    - Email…?
Pre-Authentication: The Old Switcheroo

- Easiest techniques to execute are often most effective
- Simply play the man-in-the-middle
  - Pretend to be the site a user wants
  - Get valid username/password
  - Send to legitimate site on their behalf
  - Complete MFA authentication process
  - Distract user and complete objective
- New tools to handle this attack automatically
Real-Time Phishing with Reel Phish

MFA code replay

- Two-Factor codes are often valid for 60 seconds
- Gives attackers a small (but sufficient) window to capture a code and replay it
- ReelPhish captures username, password, MFA code and replays them automatically
- Victim user gets redirected to legitimate login portal to “try again”
- https://github.com/fireeye/ReelPhish
Real-Time Phishing with ReelPhish

Workflow

1. Victim
2. Phising Page
3. Consultant
4. SMS / Push 2FA (potentially)
5. "Thank you" Page

... seconds later

Authentication

©2018 FireEye
OAuth – Clouds Apps FTW

Enhance productivity!

- Cloud service providers allow users to integrate third-party applications in order to drive synergy and enhance productivity
  - G Suite, Office 365, Box
- Once installed, the applications can access users’ data on their behalf at any time
  - Bypasses MFA requirements by design
OAuth – Apps on Apps

- Cloud providers let anyone with a (free) developer account create a third-party application
- Uses OAuth protocol for authentication
  - Malicious apps = OAuth abuse
- PwnAuth – an open-source platform to test OAuth abuse attacks
  - https://github.com/fireeye/PwnAuth
PwnAuth – Abusing Oauth

- Easy to use GUI for launching and managing Oauth abuse campaigns
- View and send email
- View files
- Contacts

```json
{
  "victims": [
    {
      "id": 11,
      "name": "Oauth Victim",
      "email": "oauthvictim@outlook.com"
    }
  ]
}
```
Pre-Authentication – What MFA Isn’t
Or - “FIND OUT WHAT YOUR HIGHSCHOOL MASCOT SAYS ABOUT YOU”

- **AVOID** common traps of “MFA”
- “Secret questions” are not so secret
  - Social media
  - Common answers
  - Popular quizzes collecting data
- PINs are better, but still fairly common
  - Just a second password
- Machine certificates can be easily stolen
Pre-Authentication – Attacking Phones

The call is coming from inside the house

- New techniques targeting phones directly
  - And becoming more common
- Intercept SMS token?
  - Make your phone my phone
  - New security measures popping up
- Intercept telecoms itself?
  - Proxy SMS… in theory
Post-Authentication

How attackers make themselves at home
Post-authentication – Surveying the Land

So you made it in – now what?

- Once attackers have access to target user account – what now?
  - How to maintain access
  - How to avoid detection

- Using pre-authentication tools gets you ONE session
  - Turning it into persistent access can be hard

- New attacker goals:
  - Gain control of (or adjust) flow of MFA authentication
  - Bury evidence
Post-authentication – Making a New Set of Keys

- First check – self-enrollment
  - New phone
  - Register new software token
- Next – duplicate?
  - Finding token seed files
- NOTE: This doesn’t always require MFA session
  - If email or SSO doesn’t require MFA…
  - … and it contains the above access/info…
  - …then you don’t have MFA anymore

https://guide.duo.com/add-device
Case Study - Abusing Self-Enrollment

When good enrollment goes bad

- Large industrial client
  - Sensitive data
  - Production processes
- MFA protecting VPN but not email
  - More common than many think
- Attackers compromised several users
  - Had access to email
  - No MFA enrolled for some users…
Case Study - Abusing Self-Enrollment

Where in the world are my employee’s SMS tokens

- Attacker proceeds to register their phones to compromised accounts
  - Few phones to many accounts
  - Now have VPN access to supplement backdoors
- Compromise of Windows environment identified
  - MFA compromise hidden until...
- Investigation identifies burner phones registered to multiple accounts
- End result:
  - Attackers booted out entirely
  - Self-enrollment disabled
Post-Exploitation
When everything that can go wrong does
Post-Exploitation – Once They Have Everything

Well, almost everything

- Getting domain admin / network admin
  - Access to all domain-joined systems
- But MFA often locks something away from even admins
- Attackers often want MFA access, even when they have admin privs
  - VPN access
  - Jumpbox servers
  - Password vaults
  - External services (SSO, web mail, etc.)
Post-Exploitation – Targeting MFA Management

Look at me, I’m the MFA admin now

- Simple solution – get MFA admin creds
- Many opportunities for backdoorin:
  - Add a new account
  - Enroll a new token for existing account
  - Enable emergency bypass
  - Disable requirement for MFA
  - Reset PIN for target accounts
Post-Exploitation – Targeting MFA Integration

Sweeping the leg

- For widespread use, MFA needs integration points
  - ADFS, proxy servers, etc.
- Exploiting operational needs
  - Stealing SSO/SAML token signing material
  - Adding user to AD MFA-excepted groups
  - Identifying existing users with MFA-exceptions
  - Exploiting “fail-open” conditions
  - Targeting the “server”, not the “app” – password vaulting

https://duo.com/docs/adfs#deployment-tip
Defending MFA
Leveling the playing field
Defense-in-Depth – Our Toolkit

**Proactive**
- Establishing a baseline
- Querying for anomalies
- Anticipating attacker methods
- Creating periodic “assessment” windows
- Defining the review process for data

**Reactive**
- Integrating MFA investigation into IR playbook
- Extending account triage to MFA
- Defining key data points and automating gathering
- Formalizing MFA remediation
Defense-in-Depth – Pre-Authentication

**Proactive**
- Limit external information
- Define MFA delivery – avoid user choice
- Use baseline to define suspicious authentication attempts
  - Failed and successful
- Train users to recognize credential phishing
  - Help Desk needs training too!

**Reactive**
- Once identifying suspicious attempts:
  - Block targets
    - Email
    - IP
    - Domain
- Consider pre-emptive blocking based on discovered tactics
Defense-in-Depth – Post-Authentication

**Proactive**
- Session timeouts
  - Limit how long an attacker has to figure out the landscape
- Control enrollment flow
- Minimize self-management
  - Integrate help desk approvals
- Harden alerting process

**Reactive**
- Terminate/revoke session
- Identify logs for:
  - SSO activities
  - Self-management/enrollment
- Blocking procedure as usual
- Reset backup codes
Defense-in-Depth – Post-Exploitation

**Proactive**
- Isolating critical assets/accounts
- Removing information leaks inside environment
- Securing “break-glass” accounts
- Alerts on MFA group adjustments

**Reactive**
- Pulling MFA management and integration logs into workflow
- MFA account reset process
- Making critical assets a necessary part of the investigation
  - Cross-reference indicators against MFA where possible
  - Don’t forget about integration/vault servers!
Conclusion

Key takeaways
Summary

- Attackers have developed strategies to circumvent or compromise MFA
- Historically, organizations have ignored extra security for these systems
- MFA is the last line of defense for critical services, ergo:
  - We have to protect MFA as a critical service
- Modern MFA defense strategy:
  - Understand how attackers view your MFA scheme
  - Map their attack strategies to your environment/implementation
  - Implement proactive measures to detect bad behavior
  - Develop reactive strategies to integrate MFA into investigation/remediation