1+1 is Not Always 2: Bypassing Multi-Factor Authentication

Jeff Hamm, Technical Director

James Hovious, Senior Consultant

Mandiant
Introduction

• Attackers commonly find themselves in situations in which they must access a resource which is guarded by a multi-factor authentication systems. There are multiple ways that attackers can accomplish this goal. This talk will present some ways in which Mandiant’s red team, as well as attackers observed by Mandiant incident responders, have bypassed MFA.

• In the presentation, a Mandiant red team consultant will present techniques used in the field to bypass MFA and a Mandiant incident response consultant will demonstrate ways to mitigate, detect, and investigate these same techniques.
Targeted Attack Life Cycle
Jeff Hamm

• IR consultant with Mandiant since 2010
  • Technical Director and IR function lead in Europe since 2014
  • Adjunct lecturer at NTNU (Norwegian University of Science and Technology) since 2011
  • Deputy Sheriff/Detective/Sergeant at Oakland County Sheriff’s Office, Michigan 1997-2008
  • Co-Author “Digital Forensics” 2017, Wiley
James Hovious

• RT consultant with Mandiant since 2015
  • EMEA Red Team Function lead
  • Does great things and will do more.
  • Will write a book in the future
  • Speaks fluent Italian so please ask lots of questions in Italian
Agenda

• Introductions
• Prerequisites
• Known Methods
  • Steal Seeds
  • Provision an Emergency Token
  • Replay Live Tokens
  • Whitelist Exceptions
  • Browser Pivot and Concurrent Sessions
  • Identify Undocumented Network Rules
• Other Methods
• Summary
Prerequisites
Prerequisites

• Keystroke Logging
  • RSA passwords usually include the use of a PIN.
  • This PIN is periodically changed according to organizational SOP plus a revolving token.
  • Attackers will typically make use of keyloggers in order to obtain the PIN.
Steal Seeds
Steal Seeds

• RSA 2FA soft tokens and mobile tokens use a seed file
  • .sdtid
  • Synched with an authentication server
  • May be reused
    • Even on separate devices
  • Can be encrypted with a password
    • Commonly the password is shared
    • The shared password may be sent over unencrypted email
  • Configured with an expiration date
• RSA tokens are commonly sent over unencrypted email
• May be stored on an SMB file server
Steal Seeds

- Attacker’s can then import the token to their device or local system.
Steal Seeds

• Prevent
  • Do not send .sdtid files via unencrypted email
  • Do not send passwords in the same medium as RSA tokens
  • Prevent duplicate tokens from operating
  • Do not use shared passwords
  • Do not store on unencrypted file servers

• Detect
  • Alert on two users logged on simultaneously with MFA

• Respond
  • Review OWA and exchange logs for “.sdtid” searches
Provision an Emergency Token
Provision an Emergency Token

• RSA Administration Server
  • Using active directory credentials for authentication
  • Domain administrator credentials
  • Access the web console
  • Generate a back up token with single factor credentials
Provision an Emergency Token

• Prevent
  • Use local credentials for RSA administrators (not AD)
  • Use one time use and password vaults for RSA administrators
  • Use a jump box to access RSA servers

• Detect
  • Alert on domain accounts logging into the RSA servers
  • Alert on account creation

• Respond
  • Review of RSA server logs
    • http logs
Replay Live Tokens
Replay Live Tokens

• Replay the full PIN + token combination
  • Keystroke logging
  • Automate alerting for opening of an MFA protected resource
Replay Live Tokens

• Prevent
  • Utilize the “push” functionality versus sending a passcode
  • Block simultaneous logins for MFA resources
• Detect
  • Alert on simultaneous logins for MFA resources
• Respond
  • Review of authentication logs
Whitelist Exceptions
Whitelist Exceptions

• Some products are configured to require MFA from all hosts except a whitelisted network or host

• Gain access to this network
  • Or configure your network to be whitelisted

Attack and Subvert
Whitelist Exceptions

• Prevent
  • Protect the whitelist with access controls

• Detect
  • Alert on any changes to the whitelist document

• Respond
  • Analyze the whitelist document
  • Event logs
Browser Pivot and Concurrent Sessions
Browser Pivot and Concurrent Sessions

- Inject into the process of an already authenticated browser session
  - Requests come from the already authenticated browser
Browser Pivot and Concurrent Sessions

• Prevent
  • No dual logins
• Detect
  • GEO alerting
• Respond
  • Browser history logs???
Identify Undocumented Network Rules
Identify Undocumented Network Rules

• Can you run `netstat` across multiple devices using:
  • Your implant?
  • Configuration management programs?
• Correlate connections to identify single factor routes into your target network
Identify Undocumented Network Rules

• Prevent
  • Ensure network segmentation
    • Host firewalls
    • Network firewalls
  • Audit network segmentation
    • Penetration testing

• Detect
  • East-west traffic

• Respond
  • Network logs
  • Event logs
Other Methods
Other Methods

• Two factor exceptions
• Machine certification as second factor
• Attack the MFA service
• Direct database access to MFA DB
• WebCam Access By MSSP?? WHAT?
  • https://www.youtube.com/watch?v=AsNwon4fjqY
Summary

• Prerequisites
• Methods
  • Steal Seeds
  • Provision an Emergency Token
  • Replay Live Tokens
  • Whitelist Exceptions
  • Browser Pivot and Concurrent Sessions
  • Identify Undocumented Network Rules
• Other Methods
Questions?

- Jeff Hamm
  - Technical Director
    - jeff.hamm@mandiant.com
    - hammjd@yahoo.com

- James Hovious
  - Senior Consultant
    - james.hovious@mandiant.com