CliftonLarsonAllen

# Beyond the Theoretical: A Practical Walkthrough of an Email Phishing Attack



# Disclaimers

*The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.*

# Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623.**

- **Q&A session will be held at the end of the presentation.**
  - Your questions can be submitted via the **Questions Function at any time during the presentation.**

- The **PowerPoint presentation,** as well as the **webinar recording,** will be sent to you within the next 10 business days.

- Please complete our online survey.

# About CliftonLarsonAllen

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting
- 3,600 employees
- Offices coast to coast
- Serve more than 1,100 financial institutions

*Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.*

# Speaker Introduction

- **David Anderson, OSCP**

  David is a manager and information security consultant with CliftonLarsonAllen. He has seven years of experience in the Information Technology field and specializes in network penetration testing, internal vulnerability assessments, and social engineering engagements.

# Learning Objectives

- At the end of this session, you will be able to:
  - Detect email phishing attacks
  - Recognize methods used by cyber criminals to penetrate networks
  - Identify best practices to protect your information assets

# Agenda

- Introduction to email phishing attacks
- Reconnaissance
- Delivering the attack
- Post-Exploitation attacks
- Remediation best practices

# Introduction to Phishing Attacks

# What is Phishing

- Simply put:
  - Convince someone to perform an action that will benefit the attacker
- What is that action?
  - Visit a malicious website
  - Download and open a malicious file
  - Provide confidential information (Password, Account Number, etc.)

# Types of attacks

- Traditional Attack (Spamming) – Attacker targets a large amount of users
- Spear Phishing – A custom message is built for a specific target
- Whaling – “C-level” executives or management is specifically targeted
- Pretext Calling

# Reconnaissance

# Reconnaissance

- Utilizing publicly available resources to discover information about your target
  - Google Hacking
  - Social Media (LinkedIn & Salesforce)
  - Domain Registration
  - whois information
  - TheHarvestor
- No packets are sent to the target network or systems!

# DEMO

Identify your target

# Delivering the Attack

# Message Delivery

- Direct interaction with targets email server
- Utilize a different organizations compromised email server
- Email Spoofing
  - Impersonate a trusted internal employee
  - Impersonate a trusted vendor

# Attack Vectors

- Payload Delivery
  - Direct user to malicious website
    - ◊ Drive-by attacks
    - ◊ Download a “Security Patch”
    - ◊ False authentication portals
  - Malicious attachment
    - ◊ Macro embedded Office document
    - ◊ Malicious executable files (.exe, .jar, .bat, etc.)

# What is a Payload

- Standard Shell
  - Windows command prompt
  - PowerShell
  - BASH shell

- Metasploit Framework
  - Meterpreter shell
    - ◊ Command prompt “on steroids”
    - ◊ Leverages the above environments in combination with pre defined scripts to automate exploitation of vulnerabilities

# DEMO

Deliver and gain access

# Post Exploitation Attacks

# Privileges Dictate the Attack

- Local Administrator rights
  - NT-Authority System
- Domain User rights
- Domain Administrator rights

# Post Exploitation Attacks

- Network enumeration via PowerShell
- Pass-the-Hash
- Authentication Token Impersonation
- Mimikatz
- Prompt for Password

# Network Enumeration

- PowerShell can be utilized to:
  - Enumerate Active Directory information
    - ◊ Users, Groups, Trusts, etc.
  - Search the network for systems where the user is granted administrative privileges
  - Determine which systems Domain Admins are logged into

# Pass-the-Hash

- Abuses Windows authentication functionality
- Does not require a clear text password to authenticate if password is valid on another system
- Screenshot shows an attacker authenticating to multiple systems with the password hash via Metasploit

# Pass-the-Hash

- How to protect your systems
  - Minimize shared passwords between systems
  - Disable network logons for local Admin accounts
  - Use a tool to randomize the password on each system
    - ◊ E.g. Local Administrator Password Solution (LAPS)

# DEMO

Pass-the-Hash

# Impersonating Tokens

- Token is like a cookie on a website
- Temporary key that can be used to identify yourself to another system
- You can impersonate a token in order to perform action as if you are that user
- Tokens can persist until a reboot
  - Can be used to masquerade as a user after they have logged off of a system

# Impersonating Tokens

- How to protect your systems
  - Check “Account is sensitive and cannot be delegated” in AD for sensitive accounts
  - Limited the number of interactive logons to a system

# DEMO

Impersonate a token

# Mimikatz

- Pulls **clear text** password from the memory of the computer
- Requires specific privileges (admin rights)

# Mimikatz

- How to protect yourself
  - Limit Admin access to systems
  - Use Host Intrusion Prevention System (HIPS)

# DEMO

Extract a password

# Prompt User For Password

- Simply opens up a window on the users desktop and asks user to enter their password
- It will keep prompting the user until they enter their correct password
- User training is the only protection

# DEMO

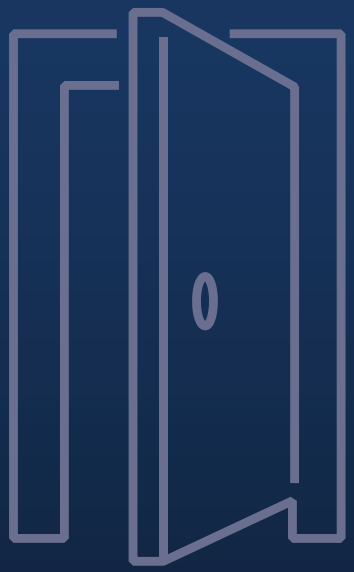
Prompt for a password

# Remediation Best Practices

# Best Practices

- Restrict Admin access as much as possible
- Disable network logons for local admin accounts
- Disable PowerShell on workstation
- Make sure systems are patched in alignment with policy
- Perform testing to validate systems are behaving as expected
- Actively train users year around on cyber security trends and threats

# Questions



# Thank you!

**David Anderson**
**Manager, Information Security Services**
**612-376-4699**
**david.anderson@CLAconnect.com**

**CLAconnect.com**