HERE TO STAY: GAINING PERSISTENCE BY ABUSING ADVANCED AUTHENTICATION MECHANISMS

MARINA SIMAKOV
IGAL GOFMAN
About Us

Marina Simakov
Security Researcher @ Microsoft

- Holds an M.Sc. in computer science
- Special interest in graph theory
- Huge dog lover

Igal Gofman
Security Researcher @ Microsoft

- Self taught security researcher & developer
- Loves Python
- Electronic music geek!
WHY ARE WE HERE?

- AWARENESS TO WEAK SPOTS
  - Relatively Easy to Exploit
  - Easily Automated
  - Usually not monitored

- DETECTION METHODS

- TALK TO US
AGENDA

- INTRODUCTION TO KEY TERMS
  - Kerberos
  - Kerberos Delegation

- GAINING PERSISTENCE
  - Focus on High Privileges
  - Malicious JIT administration

- DEMO

- MITIGATIONS & TAKEAWAYS
Ticket based authentication protocol
INTRODUCTION

• KERBEROS DELEGATION
  • Why?
    • An application reusing user credentials
    • Web server accessing a SQL DB
  • How?
    • Request tickets on behalf of the user
INTRODUCTION

DELEGATION TAB

UNCONSTRAINED DELEGATION
- Delegation to any service

CONSTRAINED DELEGATION
- Kerberos Only (S4U2Proxy)
- Protocol Transition (S4U2Self + S4U2Proxy)
GAINING PERSISTENCE
FROM ZERO TO HERO

NO ACCESS
- Domain Account
- Local System Access

PIVOTING
- Brute Force
- GPOs
- Kerberoasting

Privileged
- Pass-The-Hash
- Pass-The-Ticket
- BloodHound
- GoFetch

BUSTED!
- ACLs

FULL CONTROL
- Domain Admin
- Enterprise Admin

HERE TO STAY: GAINING PERSISTENCE BY ABUSING ADVANCED AUTHENTICATION MECHANISMS @ DEF CON
PERSISTENCE - PRIVILEGED
PERSISTENCE - PRIVILEGED

• COMMON METHODS
  • Dump NTDS.dit (VSS, DRSUAPI)
  • Golden ticket
  • Skeleton key

• WEAKNESSES
  • Replication requests from a non-DC machine
  • Detect crafted tickets
  • Encryption downgrade
JUST IN TIME ADMINISTRATION (JIT)
PERSISTENCE - PRIVILEGED

• JIT (JUST-IN-TIME) ADMINISTRATION
  • Accounts holding permanent high privileges serve as valuable targets for attackers
  • JIT Administration
    • High privileges are required to perform an operation
    • Get the required privileges for a limited amount of time
    • When the time period expires, the high privileges are revoked
  • Reduces the attack surface
PERSISTENCE - PRIVILEGED

▪ MAL-JIT (MALICIOUS-JUST-IN-TIME)
  • Get administrative access for a limited time
  • Perform malicious operations
  • Leave no traces behind to avoid detection

▪ SCENARIOS
  • Delegation scenario
  • AdminSDHolder scenario 1
  • AdminSDHolder scenario 2
MALICIOUS JIT
DELEGATION SCENARIO
PERSISTENCE - PRIVILEGED

- **OBJECTS INTRO**
  - Object Ownership
  - Discretionary Access Control List (DACL)
  - Access control entries (ACE)

LSA Matches SIDs from The access Token with SIDs in the ACEs

Access Token
- User SID
- Security Group SIDs
- User Rights

DACL
- Deny ACEs
- Allow ACEs
- Inherited Deny ACEs
- Inherited Allow ACEs

**HERE TO STAY: GAINING PERSISTENCE BY ABUSING ADVANCED AUTHENTICATION MECHANISMS @ DEF CON**
PERSISTENCE - PRIVILEGED

- DELEGATION SCENARIO
  - Add a new machine account
  - Set machine owner to a malicious account
  - Owner can edit the ACL of the object
PERSISTENCE - PRIVILEGED

- DELEGATION SCENARIO
  - GPO Tampering: “Enable accounts to be trusted for delegation”
I lost all of my administrative rights
PERSISTENCE - PRIVILEGED

- DELEGATION SCENARIO - MAL-JIT
  - DACL Modification:
    - Add ‘GenericAll’ ACE for malicious_user on new machine
DELEGATION SCENARIO - MAL-JIT

- Allow delegation to krbtgt
- Request ‘Administrator’ TGT
- Remove footprints:
  - Remove delegation
  - Revert ACL
- Perform malicious operations
MAL-JIT SUCCESSFUL!
< DEMO 1 >
MALICIOUS JIT
ADMINSDHOLDER MANIPULATION 1
PERSISTENCE - PRIVILEGED

- **ADMSNDHOLDER MANIPULATION 1**
  - Persistence can be obtained by ACL modification of privileged groups - such as ‘Domain Admins’

  ![Domain Admins Properties](image)

  - Problem: AdminSDHolder!
PERSISTENCE - PRIVILEGED

**ADMSHDHOLDER MANIPULATION 1**

- SDProp overrides the ACLs of protected groups & users with the AdminSDHolder ACL
- Runs periodically (default: 1 hour)
- Result: malicious_user loses his permission

- Protected accounts:
  - Enterprise Admins
  - Domain Admins
  - Administrators
  - ...

HERE TO STAY: GAINING PERSISTENCE BY ABUSING ADVANCED AUTHENTICATION MECHANISMS @ DEF CON
The following groups can be excluded from the AdminSDHolder protection:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Group to Exclude</th>
<th>Binary Value</th>
<th>Hexadecimal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Account Operators</td>
<td>0001</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Server Operators</td>
<td>0010</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Print Operators</td>
<td>0100</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Backup Operators</td>
<td>1000</td>
<td>8</td>
</tr>
</tbody>
</table>

Exclude groups by editing the ‘dsHeuristics’ attribute under the Configuration Container.
**PERSISTENCE - PRIVILEGED**

- **ADMSNDHOLDER MANIPULATION 1**
  - Add ACEs to excluded groups

  ![Backup Operators Properties](image)

  - SDProp will not affect the new ACL
  - Malicious JIT at any time!
MALICIOUS JIT ADMINSDHOLDER MANIPULATION 2
PERSISTENCE - PRIVILEGED

- **ADMSNDHOLDER MANIPULATION 2**
  - Change the owner of the AdminSDHolder object
  - Still not allowed to modify group memberships
Oh, No... Not Again!
PERSISTENCE - PRIVILEGED

- ADMINSĐHOLDER MANIPULATION 2 - MAL-JIT
  - Just before SDProp is scheduled to run
  - Add malicious_user to the AdminSDHolder ACL
PERSISTENCE - PRIVILEGED

- **ADMINSDDHOLDER MANIPULATION 2 - MAL-JIT**
  - SDProp adds malicious ACE to protected objects
PERSISTENCE - PRIVILEGED

• ADMINSDHOLDER MANIPULATION 2 - MAL-JIT
  • Add malicious_user to ‘Domain Admins’ group
    
    ![Windows PowerShell]
    ```powershell
    PS C:\Users\user1> Add-ADGroupMember 'Domain Admins' user1
    PS C:\Users\user1> -
    ```
    • Obtain administrative TGT
    • Revert (erase footprints)
      • Remove malicious_user from AdminSDHolder’s ACL
      • Force SDProp to run: removes malicious ACE from protected groups
      • Remove malicious_user from ‘Domain Admins’ group*
  
• Entire operation can be automated to run in seconds!
MITIGATIONS

**DETECT DELEGATION MISCONFIGURATIONS**
- ‘Account is sensitive and cannot be delegated’
- GPO: ‘Enable accounts to be trusted for delegation’
- Monitor accounts trusted for delegation
- ‘AllowedToDelegateTo’ attribute

**MONITOR ADMINSDHOLDER**
- ACL
- Owner
- Excluded groups
QUESTIONS ?