SUBORNER
A Windows Bribery for Invisible Persistence

Sebastián Castro
@r4wd3r

R4WS3C.COM
### WHOAMI

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>r4wd3r</td>
</tr>
<tr>
<td>Full User name</td>
<td>Sebastián Castro</td>
</tr>
<tr>
<td>Comment</td>
<td>Infosec nerd, stuff breaker ~10y</td>
</tr>
<tr>
<td>User’s comment</td>
<td>Terrible at MS Paint :(</td>
</tr>
<tr>
<td>First logon</td>
<td>1993/05/03 23:56</td>
</tr>
</tbody>
</table>
| User profile           | Ph. D. CSE Student <at> UCSC  
PSO R&D Co-op <at> AMD  
Presenter <at> BlackHat, BSides, Derbycon, Romhack, SEC-T... |
I, Sebastian Castro, solely and exclusively own the property rights of the research “Suborner: A Windows Bribery for Invisible Persistence”. I hereby do not concede any property rights to my previous, current and future employers unless I voluntarily choose to transfer such property, in total, or in part.

The opinions expressed here are my own and not necessarily those of my employers.
ACKNOWLEDGEMENT

This is only possible thanks to:

- Family and friends
- Research done before by great minds (Mimikatz, Impacket, etc.)
- Microsoft Team
- Stack Overflow & Infosec community. You all rock!
AGENDA

Why?

What?

How?

Show me!

What’s next?
AGENDA

Why?

What?

How?

Show me!

What’s next?
BACK IN THE DAY...

how to create invisible user windows

Google Search | I'm Feeling Lucky
BACK IN THE DAY...

I wasn’t lucky :(

how to create invisible user windows

I’m not lucky
HOW ABOUT NOW?

Google search for "how to create invisible user windows"

About 439,000,000 results (0.37 seconds)
Create Hidden Administrator User Account in Windows 11/10

```plaintext
@echo off
net user hidden yourpassword /add
net localgroup Administrators hidden /add
```
Creating a hidden user

Hi everyone,

I'm running a PC w/ Windows 10 Pro (v.2004) and is not on a domain.

I want to make my administrator account hidden from the user account screen. Instead, I want an option that says ("Other User") where I can type in the account's Username if I ever need to log in. That way, the standard users can log into this computer without having to see my Admin account's name.

Does anyone know if this is possible? Thank you in advance for any help!

I want to make my administrator account hidden

http://woshub.com/how-to-show-all-users-account...

There is no other way I know to do this than the methods shown in the tutorials.
Hi everyone,

I'm running a PC w/ Windows 10 on recent updates, and I want to make my administrator account hidden from the user account screen. Instead, I want an option that says "Other User" where I can type in the name of a saved password.

Hi Mason. I'm Greg, an installation specialist, 10 years awarded Windows MVP, and Volunteer Moderator, here to help you.

Here's how to hide a User account from the Sign-in Screen in Windows 10:
https://www.windowcentral.com/how-hide-specific...
http://woshub.com/how-to-show-all-users-account...

There is no other way I know to do this than the methods shown in the tutorials.
WHAT ABOUT ATTACKERS?

- Identity Manipulation
- External Implants

MITRE ATT&CK®
MITRE | ATT&CK®

19 persistence techniques

Reference: https://attack.mitre.org/

Account Manipulation
Create Account
Valid accounts

Identity Manipulation

External Implants

BITS Jobs
Boot or Logon Autostart Execution
Boot or Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create or Modify System Process
Event Triggered Execution
External Remote Services

Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task(Job
Server Software Components
Traffic Signaling
19 persistence techniques

Reference: https://attack.mitre.org/

Bits Jobs
Boot or Logon Autostart Execution
Boot or Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create or Modify System Process
Event Triggered Execution
External Remote Services

Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software Components
Traffic Signaling
63 of the 85 unique procedures for persistence leverage Identity Manipulation

Reference: https://attack.mitre.org/
AGENDA

Why?

What?

How?

Show me!

What’s next?
Suborner is a new persistence attack to stealthily forge custom invisible accounts which can impersonate any identity on all Windows NT machines.
THE SUBORNER WAY

- Only who created the suborner account will easily know the username and password

- After authenticated, the suborner account will impersonate any existent (enabled/disabled) account
**Suborner Account Data:**
- Username: DSKTP-WIN11-8726
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True

---

The image shows a PowerShell window with a command running, retrieving account data and creating a new account. The command being executed involves creating a new account with the specified RID and template account RID.
**SUBORNER**

**BRIBING WINDOWS**

[+] Suborner Account Data:
- Username: DSKTP-WIN11-872$
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True

[+] Crafted F key
[-] Writing V account values
[-] Encrypting password for V
[-] NTLM Hash for password: 4D33231D834E83976764DCAC18CCCD3
[+] Crafted V key
[-] Writing changes to registry
[+] The suborner account DSKTP-WIN11-872$ has been created!

PS C:\\Suborner>
GETTING US ACCESS

```bash
psexec.py DSKTP-WIN11-872$\Password.1@192.168.8.129
```

The command completed with one or more errors.
GETTING US ACCESS

```
[user@LAPTOP-50898u]~$ ~
>>> psexec.py DSKTP-WIN11-872\$:Password.1@192.168.8.129
[*] Requesting shares on 192.168.8.129......
[*] Found writable share ADMINS
[*] Opening SVCMgr on 192.168.8.129......
[*] Creating service a0CF on 192.168.8.129......
[*] Starting service a0CF......
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> whoami
nt authority\system
C:\WINDOWS\system32> net users
User accounts for \n
```

Administrator  DefaultAccount   Guest
User           WDAGUtilityAccount
The command completed with one or more errors.

```
**SUBORNER**

**GETTING US ACCESS**

```bash
>>> pseexec.py DSKTP-WIN11-872$::Password.1@192.168.8.129
```

```
C:\WINDOWS\system32> whoami
nt authority\system
```

```
C:\WINDOWS\system32> net users
User accounts for \

Administrator     DefaultAccount     Guest
user
WDAGUtilityAccount
The command completed with one or more errors.
```

---

[@r4wd3r](https://twitter.com/@r4wd3r)

R4WSEC.COM

#HITB2022SIN
WAIT A MINUTE!
BEFORE...

Attacker

Victim

Admin
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user
- Scenario 2: Add user with $
- Scenario 3: Add machine account (netapi32)
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user
- Scenario 2: Add user with $
- Scenario 3: Add machine account (netapi32)
SCENARIO #1: ADD USER

C:\>net user baddie /add
SCENARIO #1: ADD USER
SCENARIO #1: ADD USER
SCENARIO #1: ADD USER
SCENARIO #1: ADD USER
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user  FAIL!

- Scenario 2: Add user with $

- Scenario 3: Add machine account (netapi32)
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user  FAIL!

- Scenario 2: Add user with $

- Scenario 3: Add machine account (netapi32)
SCENARIO #2: ADD USER $
SCENARIO #2: ADD USER $
SCENARIO #2: ADD USER $
SCENARIO #2: ADD USER $
Scenario #2: Add User $
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user  FAIL!

- Scenario 2: Add user with $  FAIL!

- Scenario 3: Add machine account (netapi32)
ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user  FAIL!

- Scenario 2: Add user with $  FAIL!

- Scenario 3: Add machine account (netapi32)
SCENARIO #3: NETAPI32

USER_INFO_1 baddieInfo {
    usri1_name = baddie$
    ...
    usri1_priv = 1
    usri1_flags = 0x1000
}
netapi32::NetUserAdd(baddieInfo)
SCENARIO #3: NETAPI32
Scenario #3: NetAPI32

C:\>net users
User accounts for \LAPTOP
r4wadministrator
r4wguest
SCENARIO #3: NETAPI32
SCENARIO #3: NETAPI32
WHAT IS WRONG?

- The **baddie** account is detected:
  - When created (Windows Events, API Call Sequence Analysis)
  - After its creation (User Management Applications)
WHAT IS WRONG?

- The baddie account is detected:
  - When created (Windows Events, API Call Sequence)
  - After its creation (User Management Applications)

- The account needs to be added to an administrative group (e.g. Administrators)
WHAT IS WRONG?

- The baddie account is detected:
  - When created (Windows Events, API Call Sequence)
  - After its creation (User Management Applications)

- The account needs to be added to an administrative group (e.g. Administrators)

- The Win32 API impedes to modify all account attributes freely
WHAT CAN WE DO?
BRIBE IT!
SUBORNER

- NetUserAdd API
- Creds Mgmt
- LSASS
- SAM
- Event Logger
- Security Log
- LSA Policy
- Creds Mgmt

R4WSEC.COM
Create!

NetUserAdd API

Creds Mgmt

LSASS

SAM

Event Logger

Security Log

LSA Policy

Creds Mgmt

Create!

NetUserAdd API

Creds Mgmt

LSASS

SAM

Event Logger

Security Log

LSA Policy
LSASS

SAM

Event Logger

Security Log

LSA Policy

Creds Mgmt

NetUserAdd API

R 4 W S E C . C O M

@r4wd3r
NetUserAdd API -> Creds Mgmt -> LSASS -> SAM

Done!
IDEA!
WRITE THE SAM DIRECTLY!
NO LOG!
**SUBORNER**

**SUBORNING? HOW?**

- Dynamically crafts a suborner account without calling the Win32 API functions designed to do so (e.g., `netapi32::netuseradd`)
SUBORNER

SUBORNING? HOW?

- Dynamically crafts a suborner account without calling the Win32 API functions designed to do so (e.g., netapi32::netuseradd)

- Adds extra stealth to the suborner appending the dollar sign to its username ($)
SUBORNER

SUBORNING? HOW?

- Dynamically crafts a suborner account without calling the Win32 API functions designed to do so (e.g., netapi32::netuseradd)

- Adds extra stealth to the suborner appending the dollar sign to its username ($)

- Configures the account as a machine account through its Account Control Bits (ACB).
Agenda

Why?

What?

How?

Show me!

What’s next?
G O A L S

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!
GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!
**Executive**

**Security Reference Monitor (SRM)**

**Local Security Subsystem (LSASS)**

- **MSV1_0.dll**
- **SAM Service**
  - **SAM**
  - **SAM Service (samsrv.dll)**

**Credential Management**

- **WINLOGON**
- **netapi32.dll**
- **userenv.dll**
- **Others**

**LSA Policy**

- **lsasrv.dll**
- **kerberos.dll**
- **KDC (Kdcsvc.dll)**

**Event Logger**

- **RPC**
- **Security Log**

**User mode**

**Kernel mode**

- **ALPC**
- **AD Database (ntds.dll)**
- **AD Services (ntds.dll)**
- **KDC (Kdcsvc.dll)**
- **RPC**
- **Event Logger**
- **Security Log**
- **SAM Service (samsrv.dll)**
- **SAM**
- **Others**
Authentication

Local Security Subsystem (LSASS)

- LSA Service (lsasrv.dll)
- MSV1_0.dll
- SAM Service (samsrv.dll)
- SAM
- Event Logger
- Security Log
- User mode
- Kernel mode

ALPC

Executive Security Reference Monitor (SRM)

Credential Management

WINLOGON

LSA Policy

Authentication
AUTHENTICATION

Credential Management

WINLOGON

LSA Policy

Local Security Subsystem (LSASS)

LSA Service
lsasrv.dll

MSV1_0.dll

SAM Service
samsrv.dll

SAM

Event Logger

Security Log

User mode
Kernel mode

ALPC

Executive

Security Reference Monitor (SRM)

RPC
AUTHENTICATION

Local Security Subsystem (LSASS)

Credential Management

WINLOGON

LOGON SID

LSA Service
lsasrv.dll

MSV1_0.dll

SAM Service
samsrv.dll

SAM

Event Logger

Security Log

User mode

Kernel mode

ALPC

Executive

Security Reference Monitor (SRM)
AUTHENTICATION

Local Security Subsystem (LSASS)

- Credential Management
  - WINLOGON
- LSA Service
  - lsasrv.dll
- MSV1_0.dll
- SAM Service
  - samsrv.dll
- Event Logger
- Security Log
- User mode
- Kernel mode

Executive
- Security Reference Monitor (SRM)
- LSA Policy
**AUTHENTICATION**

Local Security Subsystem (LSASS)

- LSA Service: lsasrv.dll
- MSV1_0.dll
- SAM Service: samsrv.dll
- LOGON SID

Executive

Security Reference Monitor (SRM)

Kernel mode

User mode

Credential Management

WINLOGON

LSA Policy

Security Log

Event Logger

ALPC

R 4 W S E C . C O M

@r4wd3r
AUTHENTICATION

Local Security Subsystem (LSASS)

- LSA Service lsasrv.dll
- MSV1_0.dll
- LOGON SID
- SAM Service samsrv.dll
- SAM

ALPC

- Events
- Security Log
- User mode
- Kernel mode

Executive

Security Reference Monitor (SRM)

Credential Management

WINLOGON

LSA Policy

LSA

Policy

WINLOGON
AUTHENTICATION

Local Security Subsystem (LSASS)

- LSA Service (lsasrv.dll)
- MSV1_0.dll
- SAM Service (samsrv.dll)

LOGON SID

- Event Logger
- Security Log

Credential Management
- WINLOGON
- LSA Policy

Executive
- Security Reference Monitor (SRM)

ALPC

User mode
- Kernel mode


**AUTHORIZATION**

- **Local Security Subsystem (LSASS)**
  - LSA Service: lsasrv.dll
  - MSV1_0.dll

- **Security Reference Monitor (SRM)**

- **Credential Management**
  - WINLOGON

- **User mode**
  - Executive

- **Kernel mode**
  - Security Log
  - Event Logger

- **SAM**
  - Service: samsrv.dll

- **LSA Policy**
  - Policy Management

- **Executive**
  - Security Reference Monitor (SRM)
Authorization

Local Security Subsystem (LSASS)

- LSA Service
  - lsasrv.dll
- MSV1_0.dll
- LOGON SID
- LUID
- RID SIDU

ALPC

Executive

Security Reference Monitor (SRM)

Credential Management

WINLOGON

LSA Policy

SAM

Event Logger

Security Log

User mode

Kernel mode

Executive
**Authorization**

- Local Security Subsystem (LSASS)
  - LSA Service (lsasrv.dll)
  - MSV1_0.dll
  - LOGON SID
  - LUID
- Credential Management
  - WINLOGON
- LSA Policy
- ALPC
- Executive
  - Security Reference Monitor (SRM)
- Kernel mode
  - User mode
- SAM
- Event Logger
- Security Log
- User mode
- Security Reference Monitor (SRM)
GOALS

- Understand authentication/authorization for local accounts

- Create a local account writing directly to the SAM

- Make it invisible!
WHAT IS THE MINIMUM?

Username

Password

Permissions
BUT WHERE?
TRAVEL BACK TO TIME

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ab (Default)</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>F</td>
<td>REG_BINARY</td>
</tr>
<tr>
<td>ForcePasswordR...</td>
<td>REG_BINARY</td>
</tr>
<tr>
<td>ResetData</td>
<td>REG_BINARY</td>
</tr>
<tr>
<td>SupplementalCre...</td>
<td>REG_BINARY</td>
</tr>
<tr>
<td>UserPasswordHint</td>
<td>REG_BINARY</td>
</tr>
<tr>
<td>UserTile</td>
<td>REG_BINARY</td>
</tr>
</tbody>
</table>

Registry Editor:
- My Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HARDWARE
  - SAM
    - Domains
      - Accounts
        - Aliases
      - Groups
      - Users
    - SAM
      - 000001F4
      - 000001F5
      - 00000000

#HASHTAGS

@r4wd3r
<table>
<thead>
<tr>
<th></th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0008</td>
<td>03</td>
<td>00</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0010</td>
<td>12</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0018</td>
<td>08</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>1c</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0020</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0028</td>
<td>16</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0030</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0038</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0040</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0048</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0050</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0058</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0060</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0068</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0070</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0078</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0080</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0088</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0090</td>
<td>34</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0098</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00a0</td>
<td>18</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00a8</td>
<td>54</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>38</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00b0</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00b8</td>
<td>18</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00c0</td>
<td>04</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>18</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>00c8</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>14</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
</tr>
</thead>
<tbody>
<tr>
<td>0180</td>
<td>01</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0188</td>
<td>20</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>20</td>
<td>02</td>
</tr>
<tr>
<td>01c0</td>
<td>72</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>6f</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01c8</td>
<td>52</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>07</td>
</tr>
<tr>
<td>01d0</td>
<td>65</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>07</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>01e8</td>
<td>44</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01f0</td>
<td>52</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01f8</td>
<td>49</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0200</td>
<td>01</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0208</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0210</td>
<td>9d</td>
<td>c3</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0218</td>
<td>9d</td>
<td>c0</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0220</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0228</td>
<td>6a</td>
<td>6f</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0230</td>
<td>b6</td>
<td>fb</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0238</td>
<td>43</td>
<td>60</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0240</td>
<td>c4</td>
<td>53</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0248</td>
<td>0c</td>
<td>29</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0250</td>
<td>50</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0258</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0260</td>
<td>4e</td>
<td>b3</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0268</td>
<td>52</td>
<td>33</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0270</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0278</td>
<td>45</td>
<td>fa</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>0280</td>
<td>59</td>
<td>aa</td>
<td>c2</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>
V = WTF?

V size is dynamic!
int offset = 244 (0xF4); from 0xCC
int length = 18 (0x12); Unicode
int unknown = 0;
int offset = 244 (0xF4); from 0xCC
int length = 18 (0x12); Unicode
int unknown = 0;

Username: suborner$
<table>
<thead>
<tr>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Permissions</td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Full Name</td>
</tr>
<tr>
<td>Comment</td>
</tr>
<tr>
<td>User comment</td>
</tr>
<tr>
<td>Unknown entry</td>
</tr>
<tr>
<td>Home Dir</td>
</tr>
<tr>
<td>Home Dir Connect</td>
</tr>
<tr>
<td>User Logon Script Path</td>
</tr>
<tr>
<td>Profilepath</td>
</tr>
<tr>
<td>Workstations</td>
</tr>
<tr>
<td>Hours allowed</td>
</tr>
<tr>
<td>Unknown entry</td>
</tr>
<tr>
<td>LM Hash</td>
</tr>
<tr>
<td>NTLM Hash</td>
</tr>
<tr>
<td>NTLM History</td>
</tr>
<tr>
<td>LM History</td>
</tr>
</tbody>
</table>
NTLM → SUBORNER

SAM

chntpw

Impacket
REVERCEPTION!

Key → NTLM → SAM

#HITB2022SIN  @r4wd3r  R4WSEC.COM
NTLM & SAM Hash

0x01. Check if Windows 10 v1607 or greater
NTLM & SAM HASH

0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
NTLM & SAM Hash

0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
0x03. Calculate DES Key for each NTLM part
0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
0x03. Calculate DES Key for each NTLM part
0x04. Encrypt & concat each NTLM part with DES keys
NTLM & SAM Hash

0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
0x03. Calculate DES Key for each NTLM part
0x04. Encrypt & concat each NTLM part with DES keys
0x05. Calculate SAM Key
NTLM & SAM HASH

0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
0x03. Calculate DES Key for each NTLM part
0x04. Encrypt & concat each NTLM part with DES keys
0x05. Calculate SAM Key
0x06. Calculate SAM Hash (AES or MD5)
NTLM & SAM Hash

0x01. Check if Windows 10 v1607 or greater
0x02. Calculate NTLM Hash (and split it in 2 halves)
0x03. Calculate DES Key for each NTLM part
0x04. Encrypt & concat each NTLM part with DES keys
0x05. Calculate SAM Key
0x06. Calculate SAM Hash (AES or MD5)
0x07. Write changes to V
GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!
<table>
<thead>
<tr>
<th>Variable</th>
<th>00</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lockout time</td>
<td>0000</td>
<td>02</td>
<td>00</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Last logon</td>
<td>0008</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Password last set</td>
<td>0010</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Account expires</td>
<td>0018</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Last incorrect password</td>
<td>0020</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>RID copy</td>
<td>0028</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Account Bits (ACB)</td>
<td>0030</td>
<td>F4</td>
<td>01</td>
<td>00</td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>Country code</td>
<td>0038</td>
<td>10</td>
<td>02</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Invalid password count</td>
<td>0040</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>Total logons since creation</td>
<td>0048</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>

F size is fixed!
SUBORNER

F STRUCTURE

RID copy
Account Bits (ACB)

variable
- Lockout time
- Last logon
- Password last set
- Account expires

Account Bits (ACB)
- 0030 F4 01 00 00
- 0038 10 02 00 00
RID HIJACKING FTW!

RID copy

0030 F4 01 00 00
RID Hijacking

V

F

SAM
RID Hijacking
SUBORNER

BUT WAIT

THERE'S MORE
## F: ACB BITS

### Account Bits (ACB)

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0038</td>
<td>10</td>
<td>02</td>
<td>00</td>
<td>00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACB_DISABLED</td>
<td>0x0001</td>
</tr>
<tr>
<td>ACB_HOMDIRREQ</td>
<td>0x0002</td>
</tr>
<tr>
<td>ACB_PWNOTREQ</td>
<td>0x0004</td>
</tr>
<tr>
<td>ACB_TEMPDUP</td>
<td>0x0008</td>
</tr>
<tr>
<td>ACB_NORMAL</td>
<td>0x0010</td>
</tr>
<tr>
<td>ACB_MNS</td>
<td>0x0020</td>
</tr>
<tr>
<td>ACB_DOMTRUST</td>
<td>0x0040</td>
</tr>
<tr>
<td>ACB_WSTRUST</td>
<td>0x0080</td>
</tr>
<tr>
<td>ACB_SVRTRUST</td>
<td>0x0100</td>
</tr>
<tr>
<td>ACB_PWNOEXP</td>
<td>0x0200</td>
</tr>
<tr>
<td>ACB_AUTOLOCK</td>
<td>0x0400</td>
</tr>
</tbody>
</table>
### F: Account Bits (ACB)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACB_DISABLED</td>
<td>0x0001</td>
</tr>
<tr>
<td>ACB_HOMDIRREQ</td>
<td>0x0002</td>
</tr>
<tr>
<td>ACB_PWNOTREQ</td>
<td>0x0004</td>
</tr>
<tr>
<td>ACB_TEMPDUP</td>
<td>0x0008</td>
</tr>
<tr>
<td>ACB_NORMAL</td>
<td>0x0010</td>
</tr>
<tr>
<td>ACB_MNS</td>
<td>0x0020</td>
</tr>
<tr>
<td>ACB_DOMTRUST</td>
<td>0x0040</td>
</tr>
<tr>
<td>ACB_WSTRUST</td>
<td>0x0080</td>
</tr>
<tr>
<td>ACB_SVRTRUST</td>
<td>0x0100</td>
</tr>
<tr>
<td>ACB_PWNOEXP</td>
<td>0x0200</td>
</tr>
<tr>
<td>ACB_AUTOLOCK</td>
<td>0x0400</td>
</tr>
</tbody>
</table>

```c
typedef struct _USER_INFO_1 {
    LPWSTR usri1_name;
    LPWSTR usri1_password;
    DWORD usri1_password_age;
    DWORD usri1_priv;
    LPWSTR usri1_home_dir;
    LPWSTR usri1_comment;
    DWORD usri1_flags;
    LPWSTR usri1_script_path;
} USER_INFO_1, *PUSER_INFO_1, *LPUSER_INFO_1;
```
S U B O R N E R

88 .d888888b. 
d88P 88"88b 
Y88b.88 
"Y888888b. 
88"88b 
Y88b 88.88P 
"Y888888"88

= =

ACB

$$_{V}

= =

F

SAM
ACB = \{d88888b., d88P 88"88b, Y88b.88, "Y88888b., 88"88b, Y88b 88.88P, "Y888888P", 88\}

RID Hijacking

 SUBORNER

SAM
WHAT CAN WE DO?

- Create a custom account **without** the Win32 API limitations (and without calling that noisy Event Logger)
- Modify account attributes that are unchangeable through the Win32 API (s.a. RID for Primary Access Token generation)
AGENDA

Why?
What?
How?
Show me!
What’s next?
SUBORNER v1.0.1

- C# artifact to **forge** invisible accounts

- Crafts account’s SAM registry keys and values as the OS, without the limits of its API

- Works on **ALL Windows NT Machines**
SUBORNER v1.0.1: PARAMETERS

- /username: Suborner username
- /password: Suborner password
- /rid: Suborner RID
- /ridhijack: Account to impersonate
- /template: Account template for forging
- /machineaccount: Create as machine account

SUBORNER
The Invisible Account Forger by @r4wd3r v1.0.1
https://r4wsec.com
DEMO SCENARIO

Attacker Machine
192.168.8.128

Victim Machine
192.168.8.129
Microsoft Security Response Center

para Microsoft, mi

Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). We appreciate the time taken to submit this assessment.

This report appears to describe persistent attacks on a compromised machine running as SYSTEM. As such we have determined that this submission does not meet the definition of a security vulnerability for servicing.

As such, this thread is being closed and no longer monitored. We apologize for any inconvenience this may have caused.
IT’S ALL BAD?

- Although conceived as an attack, sysadmins could use this to hide privileged local accounts from unintended actors.

- Could be detected by inspection (Automated could be tricky in the future).

- Not a domain account, but definitely could be used within AD domains.
WHAT’S NEXT?

- **Totally** substitute the Win32 API for Windows Local account management!
- Discover new attack vectors of account attributes sanitized by the OS (fuzz? Bypass detection?)
- Hack Suborn the planet!
REFERENCES

- B. Delpy, Mimikatz: Benjamin Delpy (gentilkiwi) https://github.com/gentilkiwi/mimikatz/


- Ben0xa. DoucMe https://github.com/ben0xa/doucme
S U B O R N E R
A Windows Bribery for Invisible Persistence

Sebastián Castro
@r4wd3r
srcastrot