Ex0d0 Report

Benjamin Ruddy

2022-11-16

Contents

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*

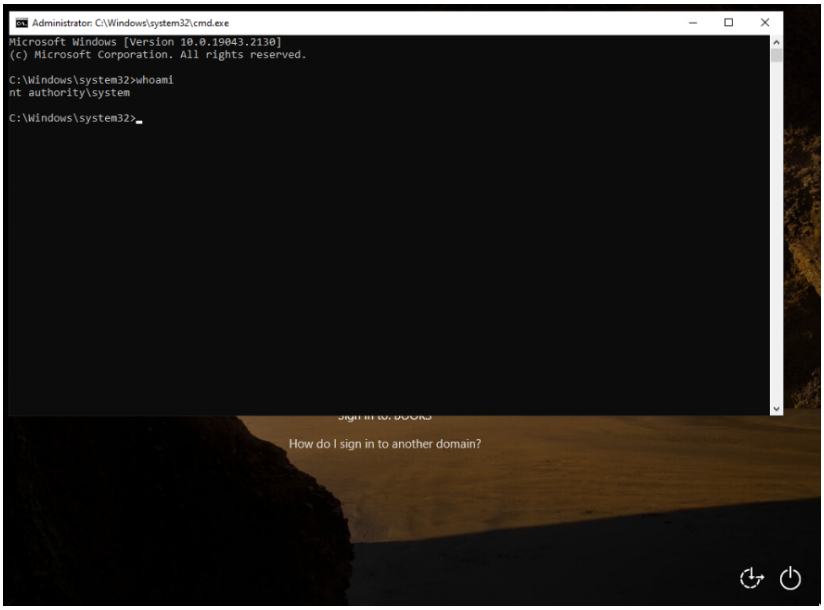
Severity Rating: 9.6

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 utilam.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*

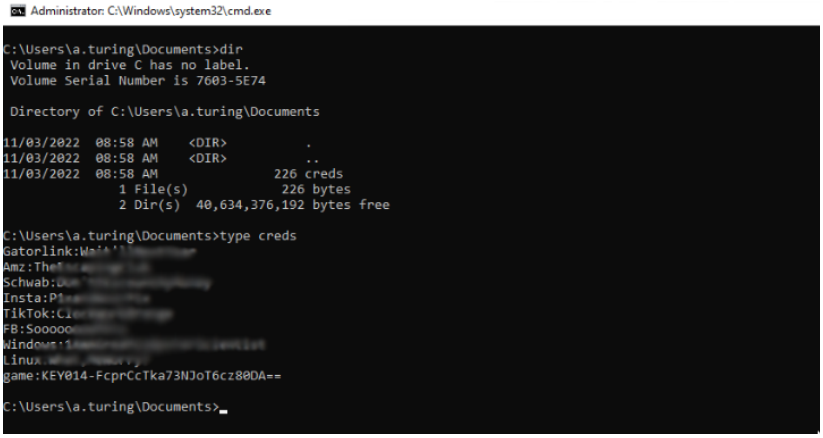
Severity Rating: 6.0

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



Mitigation or Resolution Strategy

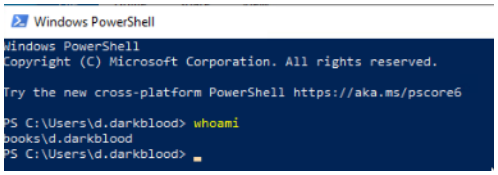
Alert the a.turing user to either opt for an encrypted, secure method of password storage (e.g. a program like KeePassXC), or simply delete the file altogether and leave password-keeping up to official administrators.

Attack Narrative

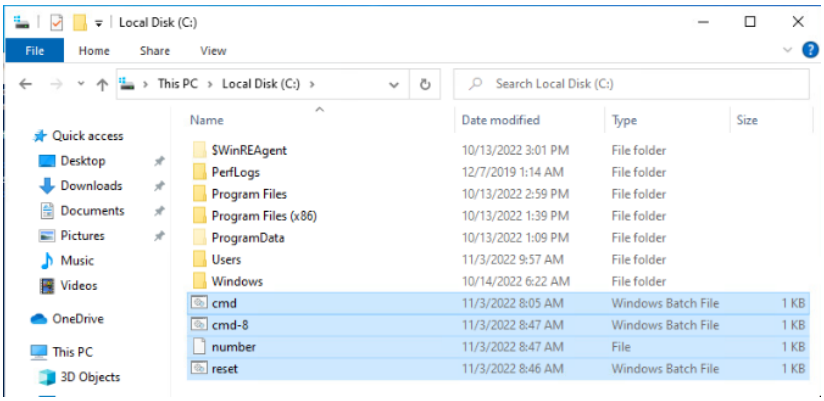
Discovering the vulnerability

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`.

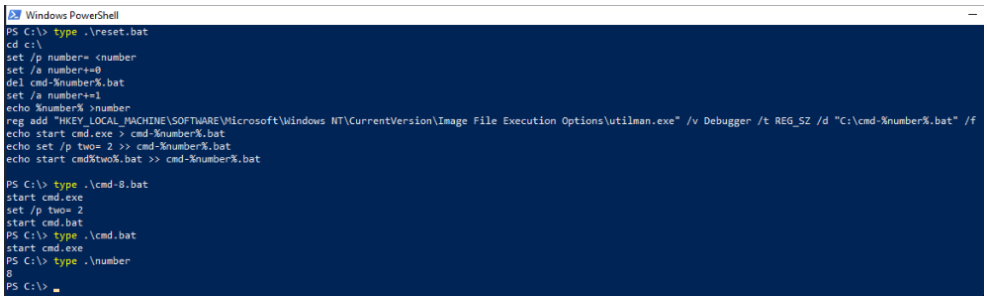
To get access, we perform the series of actions carried out in Ex0c0 and Ex090, where we copy over Chisel to `costumes.artstailor.com` through the port forward established by Hank on the innerouter, execute it through RDP, and then initiate one final RDP through proxychains to get access to books with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



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



The contents of the four highlighted files are as follows:



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 than then runs `cmd.exe` are included to fix the alleged fix that Windows 10 implemented to stop people from doing this.

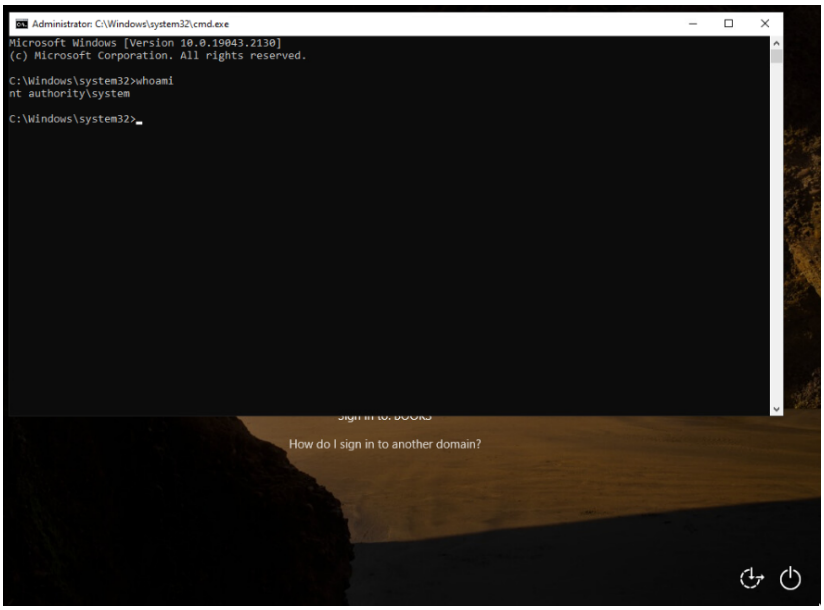
Abusing the vulnerability

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 progarm when already logged in as the d.darkblood user, but the resulting shell is not of elevated privileges:

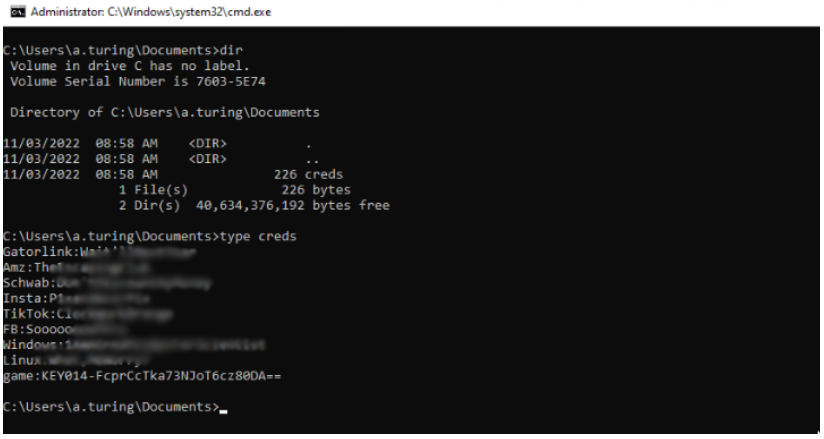
Instead, we will try to activate utilman from the logon screen by pressing the "Ease of access" icon, as suggested by https://mytekrescue.com/how-to-reset-the-password-on-almost-any-windows-computer/.

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

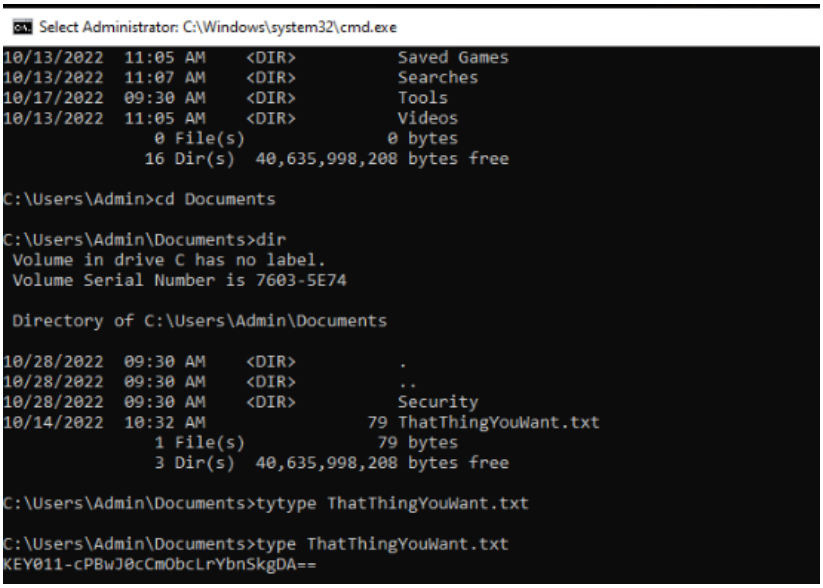


File exfiltration

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:



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:



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