Who Are We?

Eyal Itkin
Security Researcher
Check Point Research
@EyalItkin

Dana Baril
Security Researcher
Microsoft Defender ATP
@dana_baril
Motivation

- “Lazy” Lateral Movement
- “Ambush” privileged users
- IT Staff
  - Gain credentials
- Malware Researchers
  - Escape isolated virtual machines
• Collect credentials from the victim
• Attack & Take over the victim’s computer
Remote Desktop Protocol (RDP)

“Client”

• Connects to a remote Windows Machine
  o Remote corporate PC / Server
  o Local / Remote Virtual Machine

“Server”

• Attack doesn’t require “Admin”
Break `mstsc.exe`?

- PoCs from previous targets failed 😞
- The code is robust
  - Smart buffers check for parsing errors
- Includes many more features
- Where should we go now?
Back to the Drawing board

- Until now, the clipboard shared text:
  - CF_TEXT
  - CF_UNICODETEXT
- It seems like Microsoft supports many more formats now
- Let’s dig into the clipboard
Clipboard 101

- A kernel data structure that stores data
  - One clipboard per session ("connection")
  - Shared between processes

- “Caution: Clipboard data is not trusted. Parse the data carefully before using it in your application.” (MSDN)
Clipboard Over RDP

- Everything in the clipboard is synchronized automatically
- Black Lists instead of White Lists
  - Some formats are discarded by ID
  - Some formats are discarded by Name
- To avoid syncing “heavy” content, all content is subject to “delayed rendering”
Drag & Drop

• Internally, copying files is called “Drag & Drop”
• Copying files uses multiple formats
  o CF_HDROP – lists the file names
  o FileGroupDescriptorW – full metadata
  o Many more...
• Let’s see how it works in practice
Drag & Drop In Action – Ctrl+C

RDP Server

RDP client
Drag & Drop In Action – Ctrl+C

RDP Server

CF_HDROP
FGDw
ShellID
...

RDP client

FGDw
Drag & Drop In Action – Ctrl+V

RDP Server

CF_HDROP

FG Dw

RDP client
Drag & Drop In Action – Ctrl+V

- CF_HDROP
- FGDw

RDP Server

RDP client
Proprietary blob structure

Contains a list of file records
- Meta data (timestamps)
- File path – filename

Client passes it directly to the clipboard
Path Canonicalization

@GullOmer: “try to find where they sanitize the path”
Path Traversal Over RDP

- We received a CVE from Microsoft: CVE 2019-0887
- When using “Copy & Paste” a malicious server can:
  - Drop arbitrary files to arbitrary locations
- Drop your script in the Startup folder and that’s it
Taking it one step further

• The clipboards are **fully** synchronized
  o Ctrl+C updates the clipboard
  o Each update sends a `CLIPRDR_FORMAT_LIST`
  o The receiver updates his clipboard accordingly

• What does it mean?
Scenario #1 - Eavesdropping

- When the client copies a password we get it too.
- This is a **feature** of the synced clipboard.
- We know in advance when the client is going to copy a file on **his** computer.
Scenario #2 – Ctrl+V Only Attack

• Once again, ambush the client
• When he copies a file, start the attack
• Send an update message and switch his clipboard to a malicious FGDw
• His Ctrl+V will trigger the path traversal
Did we break them all?

BUT WAIT!

THERE'S MORE!
Hyper-V

• Never used it till now
• Installed a Hyper-V machine, and
Hyper-V? RDP!

- Microsoft uses RDP for accessing virtualized machines
- The GUI connection to the VM is transferred over RDP!
- Our PoC worked on the first attempt
- We just found a Guest-to-Host VM Escape 😊
Hyper-V Demo

https://youtu.be/nSGlMJqQEH0
Note on WDAG and friends

- Windows Defender Application Guard
  - Browsing “risky” sites with a virtualized Edge browser
- Uses `hvsirdpclient.exe` instead of `mstsc.exe`
- This time, MS uses White-lists instead of Black-Lists
  - Clipboard is off by default
  - The clipboard permits only 2 format types: Text & Images
- The White list blocks our vulnerability, good job ☺
VULNERABILITY DETECTED

PATCH EVERYTHING NOW!
A patch is not enough

• Users remain vulnerable until they install patch
• Detect using existing telemetry
• Detection must be implemented on “victim” machine
• RDP anomaly detection won’t cut it
Event Tracing for Windows (ETW)

- Kernel-level tracing facility that lets you log kernel or application-defined events
RDP Connections Events

Provider Guid: 1139c61b-b549-4251-8ed3-27250a1edec8
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS

Event 131 – accepting connection

Event 132 – channel connected
Clipboard Events

Non-manifested provider, tracing clipboard API usages

Provider guid: 3e0e3a92-b00b-4456-9dee-f40aba77f00e
Microsoft.Windows.OLE.Clipboard

Task name: OLE_Clipboard_MethodDiagnostics

```
ApiName:  CClipDataObject::GetData
CLIPFORMAT:  Performed DropEffect
ClipboardDataObjectTask:  0x0
HRESULT:  0x80040064
MatchFormatetc:  1
STGMEDIUM:  0x9BDA00
m_pDataObject:  0x6404478
tymed:  1
```
Clipboard Events

• Selected properties:
  o ApiName: GetData, SetData
  o CLIPFORMAT: Returned clipboard format (bitmap, text, Unicode text, etc.).
  o HRESULT: Api HResult
  o Tymed: Paste destination medium

• No clipboard content!
Telemetry Demo

https://youtu.be/nSGlMJgQ Eh0
Detection Logic – Basic

- While in RDP:
  1. When multiple files are copied in a short period of time
  2. Triggers a scan
File Creation Events

• In order to overcome the file information gap, we need more data!
• Security products have file creation indications
  o File name
  o File creation time
Detection Logic

- While in RDP:
  1. When multiple files are copied in a short period of time
  2. Correlate file creation with the same timestamps
  3. If the correlated files are in different directories – alert!
More Detection Logics

• Startup folder as a destination
  o Anomaly detection
  o Files scanning

• Clipboard as an attack vector
  o File pasting anomaly - number of pasted files or the files directories

• Malicious files dropping
  o File creation anomaly - file path, creation time and file name
OS Patch

- Verify the RDP clipboard: `ValidateFilePaths`

```c
00000016AB893FC CFormatDataPacker::DecodeFormatData(void *, ulong, uchar *, ulong)
00000016AB89646 call ?FileDescriptorW0CClipFormatTypes@@QEAAIZ
00000016AB89645 xor b4 r9d, b4 r9d
00000016AB89648 mov b4 r8d, b4 ebp
00000016AB89646 cmp b4 ebx, b4 eax
00000016AB8964D mov rdx, r14 // unsigned int
00000016AB89650 lea rax, ss:[rsp+arg_10]
00000016AB89655 setz b1 r9b // int
00000016AB89659 mov ss:[rsp+var_28], rax
00000016AB8965E call ?ValidateFilePaths@CFormatDataPacker@@AEAAJPEAKHPEAH@Z
00000016AB89663 mov b4 ebx, b4 eax
00000016AB89665 test b4 eax, b4 eax
00000016AB89667 jns 0x16AB896AD
```

- Verify canonical path before pasting:

```c
pszFilename = pCurrentFileRecord->szFilename;
status_code = PathCchCanonicalize(&pszPathOut, 0x104ui64, pszFilename);
if ((status_code & 0x80000000) != 0 ) {
```
What have we learned?

- Design lesson: Think twice before connecting different modules
  - Clipboards were designed to be used locally, and therefore trusted
  - When sharing across machines it made sense to enable clipboard sharing
  - However, this exposed machines to clipboards they can no longer trust
- Windows telemetry is an important tool in the defender’s toolbox
- Our industry can benefit from cross-community collaborations
That’s all folks

Remote Desktop Connection

Your Remote Desktop session has ended, possibly for one of the following reasons:

The administrator has ended the session.
An error occurred while the connection was being established.
A network problem occurred.

For help solving the problem, see “Remote Desktop” in Help and Support.