Poisoned RDP
He Said, She Said – Poisoned RDP Offense and Defense
Who Are We?

Eyal Itkin
Security Researcher
Check Point Research

Dana Baril
Security Researcher
Microsoft Defender ATP

@dana_baril
BlueKeep?

• A different vulnerability in the Remote Desktop Protocol
  o Unauthenticated RCE in Microsoft’s RDP Servers
  o Disclosed by the UK national CERT in May 2019

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability
Security Vulnerability
Published: 05/14/2019

• We are going to focus on a different attack vector
Motivation

• Lazy Lateral Movement
• “Ambush” privileged users
• IT Staff
  o Gain credentials
• Malware Researchers
  o Escape isolated virtual machines
Remote Desktop Protocol (RDP)

“Client”
- Connects to a remote Windows Machine
  - Remote corporate PC/Server
  - Local/Remote Virtual Machine
- A.K.A. mstsc
- Attack doesn't require "Admin"
Poisoned RDP?

- Collect credentials from the victim
- Attack & Take over the victim’s computer
RDP Clients

Remote Desktop Connection

Do you trust this remote connection?

This remote connection could harm your local or remote computer. Make sure that you trust the remote computer before you connect.

- **Type:** Remote Desktop Connection
- **Remote computer:** [redacted]

- [ ] Don't ask me again for connections to this computer

Connect  Cancel

Show Details
Our Targets

- Open Source RDP Clients
  - rdesktop
  - FreeRDP

- Microsoft’s default client
  - mstsc.exe
1. Start with the easiest target

- Pick the simplest open source - rdesktop
- Audit the code and learn how RDP works
- Find potentially vulnerable features / modules
- Gradually gain confidence
- Move on when scanned all of the code
Lessons on RDP

• Protocol consists of logical channels
  ○ BlueKeep exploits the internal (non-public) MS_T120 channel

• Contains multiple authentication methods

• Screen updates are sent using Bitmaps

• Basic Clipboard types are shared
2. Break rdesktop

- Naïve C code with less than minimal checks
  - Almost no checks that minimal input was received
- Found 11 critical vulnerabilities (19 Overall)
- CVEs:
  - CVE 2018-8791 – CVE 2018-8800
  - CVE 2018-20174 – CVE 2018-20182
3. Find complicated features

- CVE 2018-8795: Integer-Overflow in Bitmap Parsing

```c
in_uint16_le(s, width) 16 bits: 0x8000
in_uint16_le(s, height) 16 bits: 0x8001
in_uint16_le(s, bpp) 16 bits: 4

// Allocate space > 32 bits: 0x20000

bmpdata = xmalloc(width * height * bpp)

bitmap_decompress(bmpdata, width, height, bpp);
```
4. Break FreeRDP

- The C code looks better
  - Still has a few cracks if we look deep enough
  - Again, vulnerable to Bitmap parsing
- Found 5 critical vulnerabilities (6 Overall)
- CVEs:
  - CVE 2018-8784 – CVE 2018-8789
mstsc.exe

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mstsc

OK  Cancel  Browse...
5. 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:
  o CF_TEXT
  o 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
  o One clipboard per session ("connection")
  o Shared between processes
• Stores data (blobs) by ID / Name
• Caution: Clipboard data is not trusted. Parse the data carefully before using it in your application.
Clipboard 101

- A kernel data structure that stores data
  - One clipboard per session (“connection”)
  - Shared between processes
- Stores data (blobs) by ID / Name
- "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
  - CF_HDROP – lists the file names
  - FileGroupDescriptorW – full metadata
  - Many more...
- Let’s see how it works in practice
Drag & Drop In Action – Ctrl+C

RDP Server

RDP client

CF_HDROP
FGDw
ShellID
...
Drag & Drop In Action – Ctrl+C

RDP Server

RDP client
Drag & Drop In Action – Ctrl+V

- RDP Server
- CF_HDROP
- FGDw
- RDP client
Drag & Drop In Action – Ctrl+V

RDP Server

RDP client
Drag & Drop In Action – Ctrl+V

RDP Server

FGDw

RDP client
Drag & Drop In Action – Ctrl+V

RDP Server

RDP client

FGDw
FileGroupDescriptorW

- 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
  - Ctrl+C updates the clipboard
  - Each update sends a `CLIPRDR_FORMAT_LIST`
  - 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
  o 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
  o Clipboard is off by default
    o The clipboard permits only 2 format types: Text & Images
• The White list blocks our vulnerability, good job 😊
Defense
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

Events 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

Message/PartC

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

- **Selected properties:**
  - ApiName: GetData, SetData
  - CLIPFORMAT: Returned clipboard format (bitmap, text, Unicode text, etc.).
  - HRESULT: Api HResult
  - Tymed: Paste destination medium
- **No clipboard content!**
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
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**

- Verify canonical path before pasting:

```c
pszFilename = pCurrentFileRecord->szFilename;
status_code = PathCchCanonicalize(&pszPathOut, 0x104u64, 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.

OK  Help