A Game of “Cut and Mouse”

Bypassing Antivirus by Simulating User Inputs

Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra

ACSAC’19, San Juan

December 11, 2019
Indispensable for Security: Antivirus Software

- The first security recommendation
  - Install an AV software

- Main defense approach: **blacklisting**
  - Signatures of malicious programs
  - Blocks known malware
Mandatory Integrity Control (MIC):

- Protect processes from malicious modifications, e.g., code injection
- Each process has an Integrity Level
  - Four levels: Low, Medium, High, System
- MIC prevents modifications if the target process has higher IL.
  - For example: `CreateRemoteThread` or `WriteProcessMemory` calls fail.

User Interface Privilege Isolation (UIPI):

- Blocks window messages from processes that have lower IL.
  - For example, `SendMessage` or `SendInput` calls fail.
Simulating User Actions

**SendInput** synthesizes keystrokes, mouse motions, and mouse clicks.

- `SendInput(MOUSE_MOVE, (x,y));`
Simulating User Actions

`SendInput` synthesizes keystrokes, mouse motions, and mouse clicks.

- `SendInput(MOUSE_MOVE, (x,y));`
- `SendInput(MOUSE_LEFTCLICK);`
Simulating User Actions

SendInput synthesizes keystrokes, mouse motions, and mouse clicks.

- `SendInput(MOUSE_MOVE, (x,y));`
- `SendInput(MOUSE_LEFTCLICK);`
- `SendInput(KEYDOWN, 'A');`
• Configuration GUIs of AVs suggest anti-rw modules are based on whitelists.

• Contains protected folders and trusted processes.

• MS also added **Controlled Folder Access** feature in Windows 10 v1709.

• Common folders in the profile folder is protected by default.

• Whitelist is maintained by AV vendor, but user can also add specific applications.
Research Questions

- **RQ1**: Can ransomware use benign applications to bypass AV?

- **RQ2**: Can malware simulate user actions and disable AV protection?
Disharmony Between UIPI and AVs

(a) Malware vs UIPI.

(b) Malware vs AV.

(c) Malware can control trusted applications to overwrite protected files.
Cut-and-Mouse: Encrypting Protected Files

- Ransomware
- Run Window
- Protected Files
- Windows Clipboard
- Trusted Application e.g., Notepad
Cut-and-Mouse: Encrypting Protected Files

Ransomware

1. Read File Contents

Protected Files

Windows Clipboard

Run Window

Trusted Application e.g., Notepad
Cut-and-Mouse: Encrypting Protected Files

1. **Ransomware**
   - Read File Contents

2. **Copy to Clipboard**

   - **Protected Files**

   - **Windows Clipboard**

   - **Trusted Application** e.g., Notepad

   - **Run Window**
Cut-and-Mouse: Encrypting Protected Files

1. Read File Contents
2. Copy to Clipboard
3. Open Run Window

Ransomware → Protected Files → Windows Clipboard → Trusted Application e.g., Notepad
Cut-and-Mouse: Encrypting Protected Files

1. Read File Contents
2. Copy to Clipboard
3. Open Run Window
4. Launch Notepad

Ransomware

Protected Files

Windows Clipboard

Trusted Application e.g., Notepad
Cut-and-Mouse: Encrypting Protected Files

1. Read File Contents
2. Copy to Clipboard
3. Open Run Window
4. Launch Notepad
5. Paste to Notepad
Cut-and-Mouse: Encrypting Protected Files

1. Read File Contents
2. Copy to Clipboard
3. Open Run Window
4. Launch Notepad
5. Paste to Notepad
6. Save & Close File

Ransomware
Protected Files
Run Window
Notepad
Windows Clipboard
Trusted Application e.g., Notepad
Experimental Results: Cut-and-Mouse vs AVs

- Test Environment: VMs running Windows 10 Pro x64 Version 1903, fully up-to-date.

- Collected AV software according to AV-TEST reports.

- Tested against 13 “Top Products” for Windows platform.

- Used Notepad to overwrite the files.

- Cut-and-Mouse could encrypt all files in protected folders in all of the tests.
Open ACME Antivirus GUI
SendInput(MOUSE_MOVE, (156, 247));
SendInput(MOUSE_LEFTCLICK);
Ghost Control: Disable Real-Time Protection of AVs

SendInput(MOUSE_MOVE, (225, 137));
SendInput(MOUSE_LEFTCLICK);
Ghost Control: Disable Real-Time Protection of AVs

SendInput(MOUSE_MOVE, (307, 293));
SendInput(MOUSE_LEFTCLICK);
Ghost Control: Disable Real-Time Protection of AVs

SendInput(MOUSE_MOVE, (309, 286));
SendInput(MOUSE_LEFTCLICK);
Experimental Results: Ghost Control vs AVs

- Test Environment: VMs running Windows 10 Pro x64 Version 1903, fully up-to-date.
- Collected AV software according to AV-TEST reports.
- Tested against 13 “Top Products” for Windows platform.
- Ghost Control could disable real-time protection of 6 out of 13 AVs.
- According to OPSWAT, the market share of the vulnerable AVs is more than 23%.
Discussion

- Secure Composability issue between UIPI and AVs.

- Vital to control message flow between security critical components.

- Checking Integrity Levels is not sufficient to provide security on message flow.

SECURITY PRINCIPLE: Messages between applications should be allowed only when

- the sender has at least the same integrity level as the receiver,

   AND

- the sender is at least as trusted as the receiver.
Comparison with Previous Work

Shatter Attack:
Malicious Code Injected

Cut-and-Mouse
Target Process is Intact
Conclusions

- Antivirus is the primary security tool against malware
- Surprising findings:
  - Ghost Control could easily disable several AVs
  - Cut-and-Mouse could bypass all AVs
- Message flow should be controlled with great care
- OS and AV defenses should cooperate better
A Game of “Cut and Mouse”: Bypassing Antivirus by Simulating User Inputs

ziya.genc@uni.lu