Recorded Future®
Sandbox

Malware Analysis Report

2025-10-11 15:34

Sample ID	251010-15wpwawyaw
Target	hier_officeFontsPreview_4_42.ttf
SHA256	4c41e4bc290496111489622fb119392b393b2a61f3b588f64c65ebd4368ed7db
Tags	

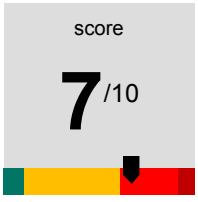


Table of Contents

Part 1. Analysis Overview

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Part 3. Analysis: static1

3. 1. Detonation Overview

3. 2. Signatures

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

4. 2. Command Line

4. 3. Signatures

4. 4. Processes

4. 5. Network

4. 6. Files

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

5. 2. Command Line

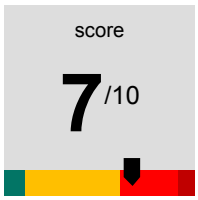
5. 3. Signatures

5. 4. Processes

5. 5. Network

5. 6. Files

Part 1. Analysis Overview



SHA256
4c41e4bc290496111489622fb119392b393b2a61f3b588f64c65ebd4368ed7db

Threat Level: Shows suspicious behavior

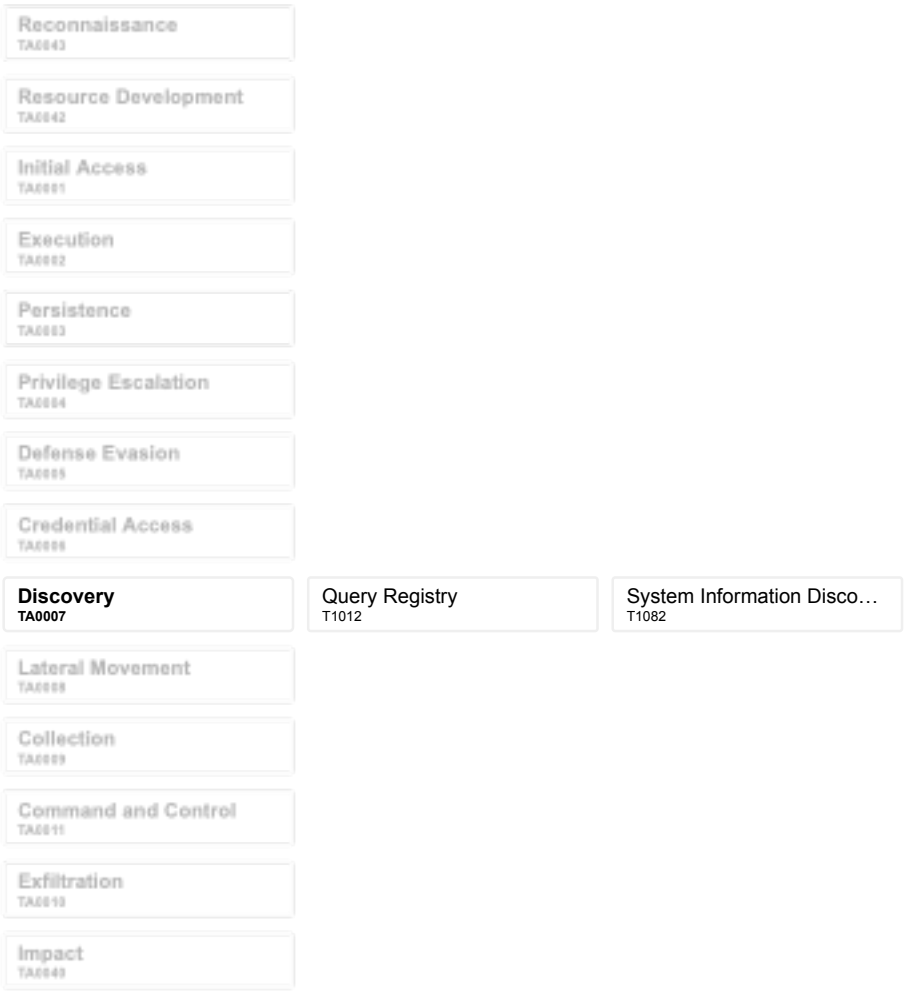
The file hier_officeFontsPreview_4_42.ttf was found to be: Shows suspicious behavior.

Malicious Activity Summary

- **Checks computer location settings**
- **Enumerates physical storage devices**
- **Modifies registry class**
- **Suspicious use of WriteProcessMemory**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16



Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-10 22:14

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-10 22:14	2025-10-10 22:17	win10v2004-20250619-en	149s	150s

4. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

4. 3. Signatures

Checks computer location settings

Description	Indicator	Process	Target
Key value queried	\REGISTRY\USER\S-1-5-21-3008489981-1977616533-741913813-1000\Control Panel\International\Geo\Nation	C:\Windows\system32\cmd.exe	N/A

Enumerates physical storage devices

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-3008489981-1977616533-741913813-1000_Classes\Local Settings	C:\Windows\system32\cmd.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 384 wrote to memory of 1988	N/A	C:\Windows\system32\cmd.exe	C:\Windows\System32\fontview.exe
PID 384 wrote to memory of 1988	N/A	C:\Windows\system32\cmd.exe	C:\Windows\System32\fontview.exe

4. 4. Processes

C:\Windows\system32\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

C:\Windows\System32\fontview.exe

```
"C:\Windows\System32\fontview.exe" C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp

4. 6. Files

C:\Users\Admin\AppData\Local\Microsoft\Windows\Fonts\hier_officeFontsPreview_4.ttf

MD5	fc535e45902a11516430770d47ed4183
SHA1	32ee7d71c2a7916d05f02b20e2d971198adb0c79
SHA256	4c41e4bc290496111489622fb119392b393b2a61f3b588f64c65ebd4368ed7db
SHA512	9781465e1655a72ce927615e45ef2b66001cd0946c26190b40b990bcb1f3228fc838218e69054136aa6b3cc9a0224eed1c91b81f5c4491678c6b5c127f249cce

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-10 22:14	2025-10-10 22:17	win11-20250502-en	149s	104s

5. 2. Command Line

```
cmd /c C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

5. 3. Signatures

Enumerates physical storage devices

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-330179853-1108322181-418488014-1000_Classes\Local Settings	C:\Windows\system32\cmd.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 2192 wrote to memory of 1952	N/A	C:\Windows\system32\cmd.exe	C:\Windows\System32\fontview.exe
PID 2192 wrote to memory of 1952	N/A	C:\Windows\system32\cmd.exe	C:\Windows\System32\fontview.exe

5. 4. Processes

C:\Windows\system32\cmd.exe

```
cmd /c C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

C:\Windows\System32\fontview.exe

```
"C:\Windows\System32\fontview.exe" C:\Users\Admin\AppData\Local\Temp\hier_officeFontsPreview_4_42.ttf
```

5. 5. Network

5. 6. Files

C:\Users\Admin\AppData\Local\Microsoft\Windows\Fonts\hier_officeFontsPreview_4.ttf

MD5	fc535e45902a11516430770d47ed4183
SHA1	32ee7d71c2a7916d05f02b20e2d971198adb0c79
SHA256	4c41e4bc290496111489622fb119392b393b2a61f3b588f64c65ebd4368ed7db
SHA512	9781465e1655a72ce927615e45ef2b66001cd0946c26190b40b990bcb1f3228fc838218e69054136aa6b3cc9a0224eed1c91b81f5c4491678c6b5c127f249cce