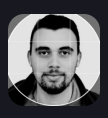
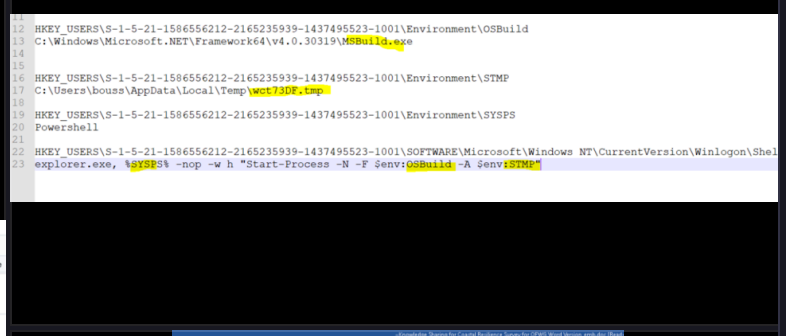


sbousseaden
@sbousseaden@infosec.exchange

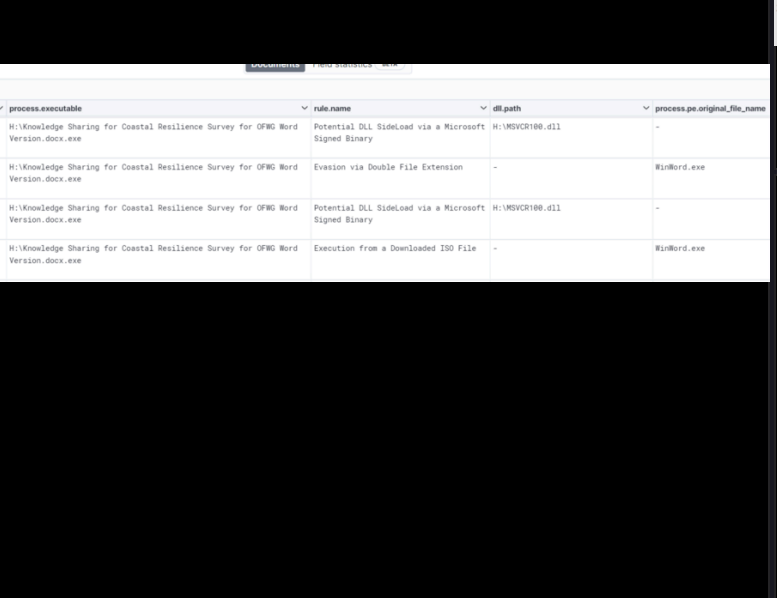
weird ISO sample, contains renamed winword.exe used to sideload MSVCR100.dll which just sets persistence via winlogon_shell & a bunch of envars to obfuscate things (cache file wct73DF.tmp is not dropped!)

bcb7e369adf827fb23521c60b7a29486a267bfe4fa11ee4de8dccb3328e2dc0f

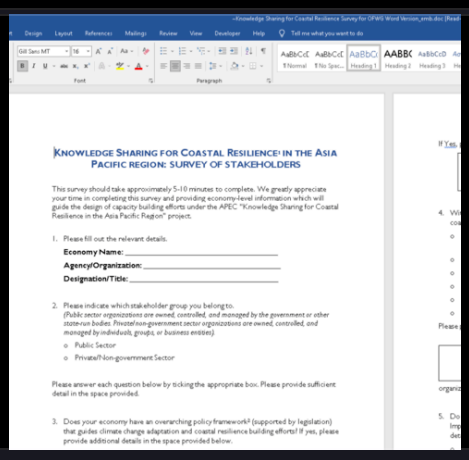
Hide



```
HKEY_USERS\S-1-5-21-1586556212-2165235939-1437495523-1001\Environment\OSBuild
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe

HKEY_USERS\S-1-5-21-1586556212-2165235939-1437495523-1001\Environment\STMP
C:\Users\bouss\AppData\Local\Temp\wct73DF.tmp

HKEY_USERS\S-1-5-21-1586556212-2165235939-1437495523-1001\Environment\SYSPS
Powershell

HKEY_USERS\S-1-5-21-1586556212-2165235939-1437495523-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shel
explorer.exe, %SYSPS% -nop -w h "Start-Process -N -F $env:OSBuild -A $env:STMP"
```



process.executable	rule.name	dll.path	process.pe.original_file_name
H:\Knowledge Sharing for Coastal Resilience Survey for OFWG Word Version.docx.exe	Potential DLL SideLoad via a Microsoft Signed Binary	H:\MSVCR100.dll	-
H:\Knowledge Sharing for Coastal Resilience Survey for OFWG Word Version.docx.exe	Evasion via Double File Extension	-	WinWord.exe
H:\Knowledge Sharing for Coastal Resilience Survey for OFWG Word Version.docx.exe	Potential DLL SideLoad via a Microsoft Signed Binary	H:\MSVCR100.dll	-
H:\Knowledge Sharing for Coastal Resilience Survey for OFWG Word Version.docx.exe	Execution from a Downloaded ISO File	-	WinWord.exe



KNOWLEDGE SHARING FOR COASTAL RESILIENCE[1] IN THE ASIA PACIFIC REGION: SURVEY OF STAKEHOLDERS

This survey should take approximately 5-10 minutes to complete. We greatly appreciate your time in completing this survey and providing economy-level information which will guide the design of capacity building efforts under the APEC "Knowledge Sharing for Coastal Resilience in the Asia Pacific Region" project.

1. Please fill out the relevant details.
   Economy Name: _____
   Agency/Organization: _____
   Designation/Title: _____

2. Please indicate which stakeholder group you belong to.
   (Public sector organizations are owned, controlled, and managed by the government or other state-run bodies. Private/non-government sector organizations are owned, controlled, and managed by individuals, groups, or business entities).
   - o Public Sector
   - o Private/Non-government Sector

Please answer each question below by ticking the appropriate box. Please provide sufficient detail in the space provided.

3. Does your economy have an overarching policy framework[2] (supported by legislation) that guides climate change adaptation and coastal resilience building efforts? If yes, please provide additional details in the space provided below.

Dec 19, 2022, 09:35 PM · · Web

4 boosts · **11** favorites