PoorTry Windows driver evolves into a full-featured EDR wiper

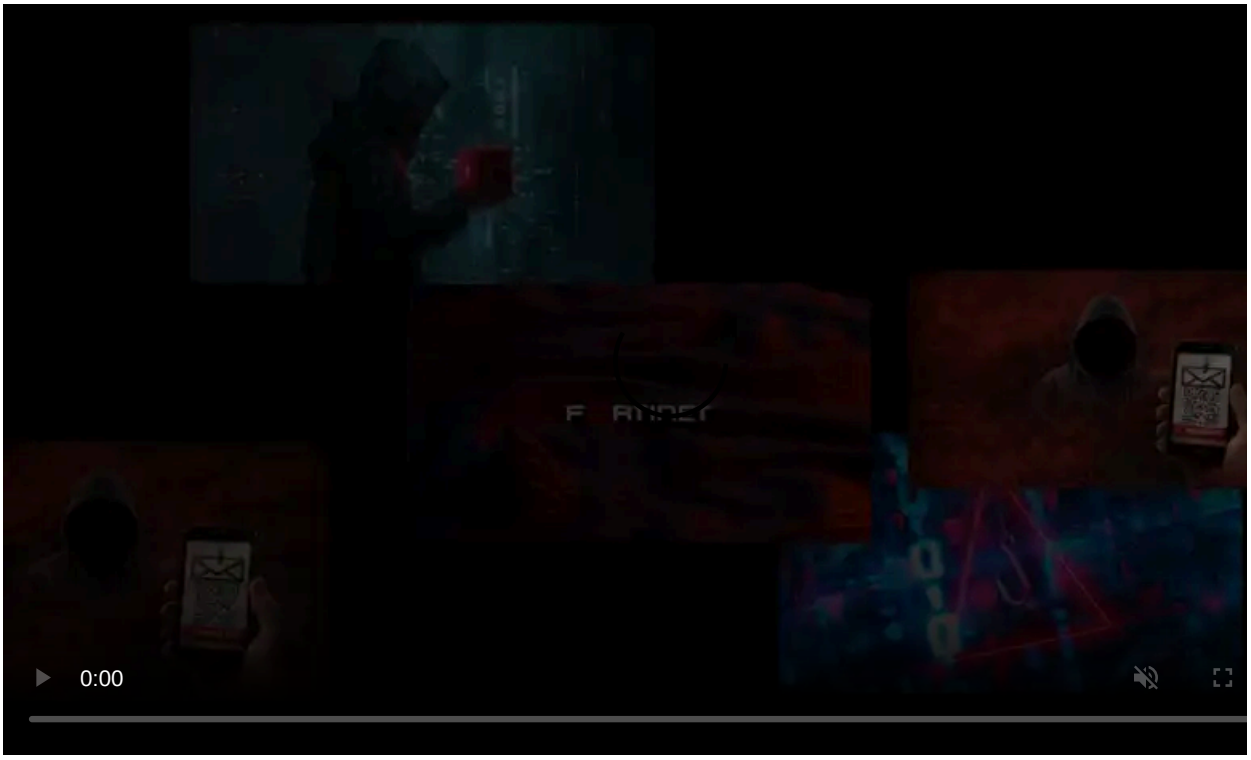
By Bill Toulas

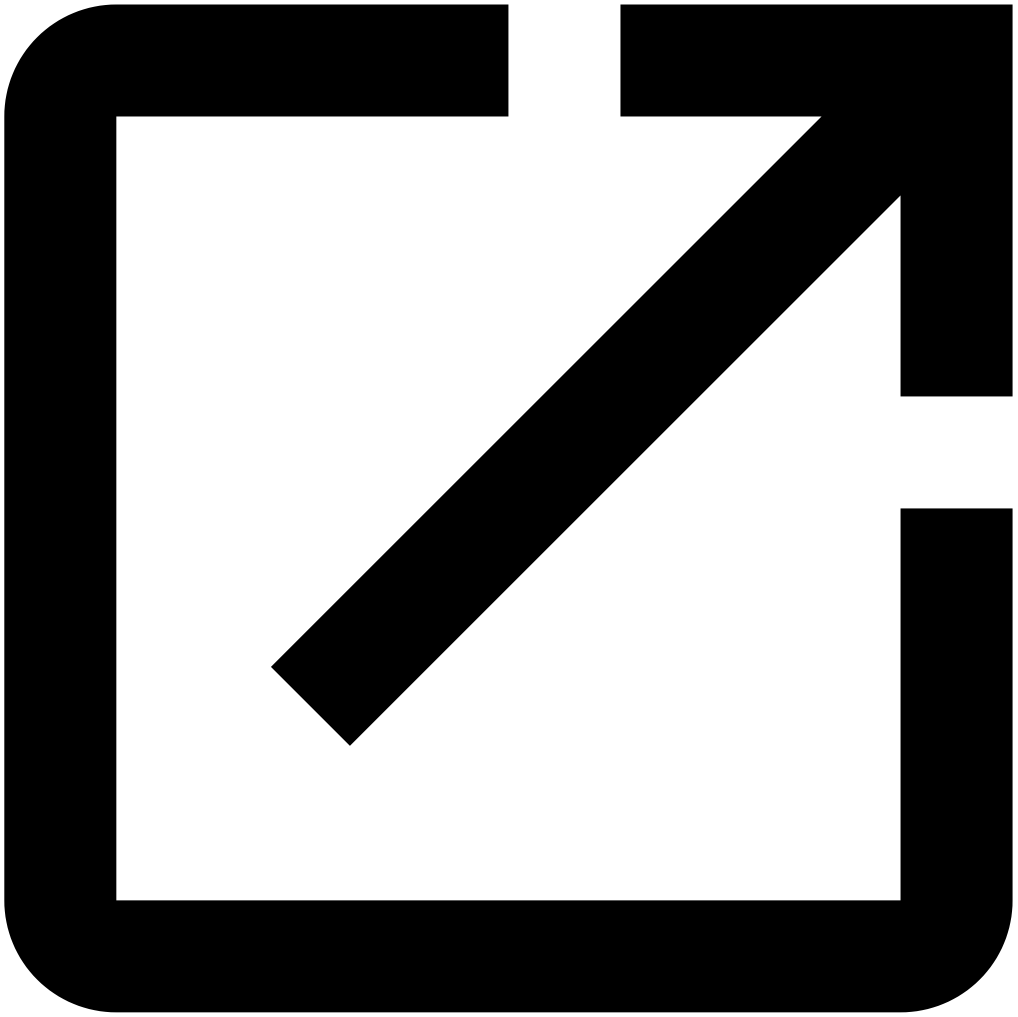
Published: 2024-08-28 · Archived: 2026-04-05 21:56:25 UTC

The malicious PoorTry kernel-mode Windows driver used by multiple ransomware gangs to turn off Endpoint Detection and Response (EDR) solutions has evolved into an EDR wiper, deleting files crucial for the operation of security solutions and making restoration harder.

Though Trend Micro had warned about this functionality added on Poortry since May 2023, Sophos has now confirmed seeing the EDR wiping attacks in the wild.

This evolution of PoorTry from an EDR deactivator to an EDR wiper represents a very aggressive shift in tactics by ransomware actors, who now prioritize a more disruptive setup phase to ensure better outcomes in the encryption stage.


0:00



PoorTry, also known as 'BurntCigar,' was developed in 2021 as a kernel-mode driver to disable EDR and other security software.

The kit, used by several ransomware gangs, including BlackCat, Cuba, and LockBit, first gained attention when its developers found ways to get their malicious drivers signed through Microsoft's attestation signing process. Other cybercrime groups, such as Scattered Spider, were also seen utilizing the tool in breaches focused on credential theft and SIM-swapping attacks.

Throughout 2022 and 2023, Poortry continued to evolve, optimizing its code and using obfuscation tools like VMProtect, Themida, and ASMGuard to pack the driver and its loader (Stonestop) for evasion.

Evolution to a wiper

The latest report by Sophos is based on a RansomHub attack in July 2024 that employed Poortry to delete critical executable files (EXEs), dynamic link libraries (DLLs), and other essential components of security software.

This ensures that EDR software cannot be recovered or restarted by defenders, leaving the system completely unprotected in the following encryption phase of the attack.

The process starts with the user-mode component of PoorTry, identifying the security software's installation directories and the critical files within those directories.

It then sends requests to the kernel-mode component to systematically terminate security-related processes and then delete their crucial files.

Paths to those files are hardcoded onto PoorTry, while the user-mode component supports deletion either by file name or type, giving it some operational flexibility to cover a broader range of EDR products.

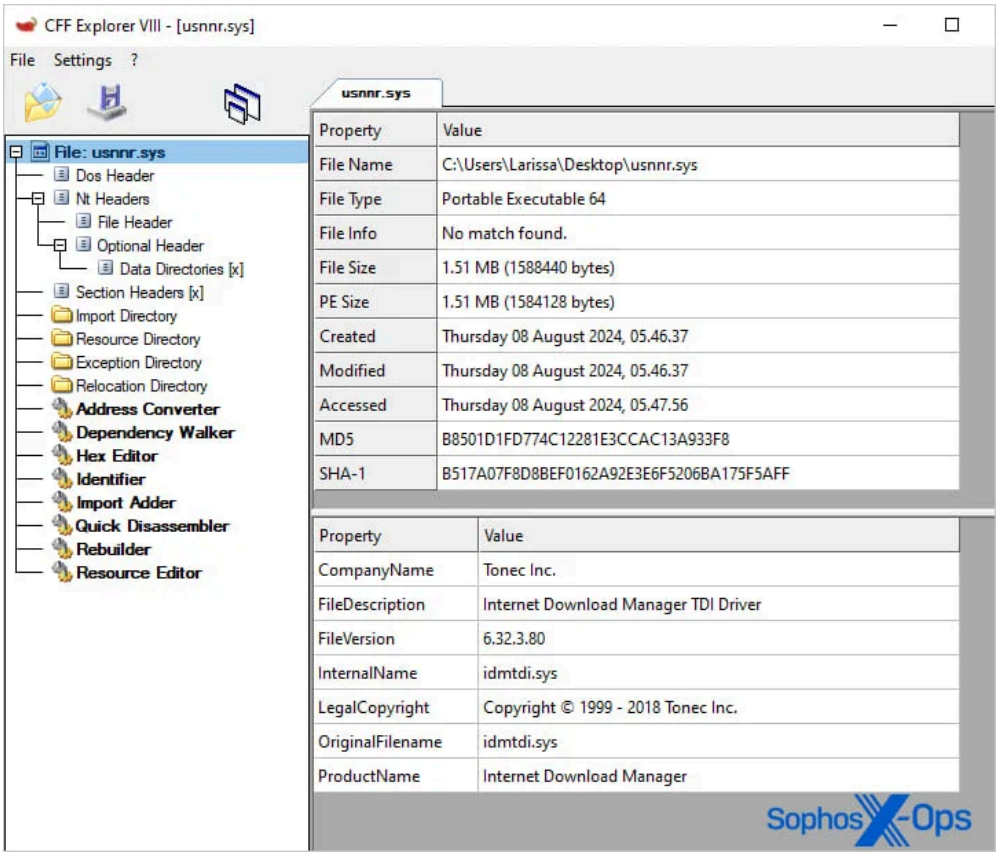
```
int __cdecl SK_ForceDeleteTypedFilesInDirByPath(int input_wsprintfW, wchar_t *configuredFileExt)
{
  const wchar_t *currFileExt; // eax
  WCHAR FileName[260]; // [esp+40h] [ebp-66Ch] BYREF
  int v6[130]; // [esp+248h] [ebp-464h] BYREF
  struct _WIN32_FIND_DATAW FindFileData; // [esp+450h] [ebp-25Ch] BYREF
  HANDLE hFindFile; // [esp+6A0h] [ebp-Ch]

  memset(FileName, 0, sizeof(FileName));
  wsprintfW(FileName, &off_40509C, input_wsprintfW);
  hFindFile = FindFirstFileW(FileName, &FindFileData);
  if ( hFindFile == (HANDLE)-1 )
    return 1;
  // Loop start, iterating through files in folder
  do
  {
    if ( lstrcmpW(FindFileData.cFileName, ".") && lstrcmpW(FindFileData.cFileName, ".") )
    {
      memset(v6, 0, sizeof(v6));
      j_memset(v6, 0, 260);
      wsprintfW(v6, &off_4050B0, input_wsprintfW);
      if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
      {
        SK_ForceDeleteTypedFilesInDirByPath((int)v6, configuredFileExt);
      }
      else
      {
        // Get file extension. If file extension equals targeted fileExt, delete file via sending iocode 0x222180 request to driver
        currFileExt = GetFileExtension(FindFileData.cFileName);
        if ( !wcsicmp(currFileExt, configuredFileExt) )
        {
          j_wprintf(L"[*] [SK_ForceDeleteTypedFilesInDirByPath] Found [%ws]\n", FindFileData.cFileName);
          Do_DeleteFile_Irp(v6);
        }
      }
    }
  }
  while ( FindNextFileW(hFindFile, &FindFileData) );
```

Deleting by file type functionality
source: Sophos

The malware can be fine-tuned only to delete files crucial to the EDR's operation, avoiding unnecessary noise in the risky first phases of the attack.

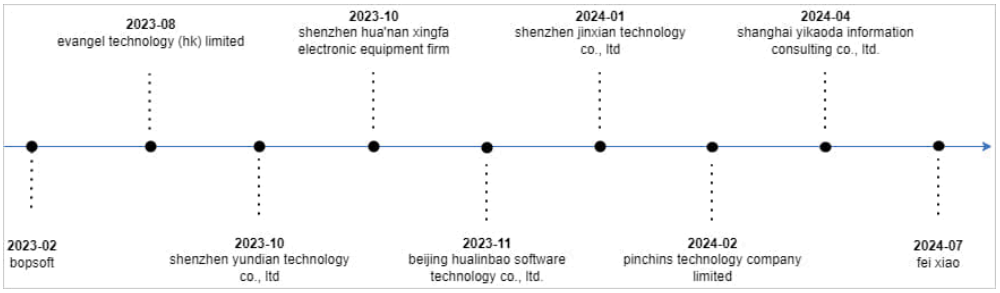
Sophos also notes that the latest Poortry variants employ signature timestamp manipulation to bypass security checks on Windows and use the metadata from other software like Internet Download Manager by Tonec Inc.



Driver properties

source: Sophos

The attackers were seen employing a tactic known as "certificate roullete," where they deploy multiple variants of the same payload signed with different certificates to increase their chances that at least one will execute successfully.



Various certificates used for signing the Poortry driver over time

source: Sophos

Despite efforts to track PoorTry's evolution and stop its effectiveness, the developers of the tool have shown a remarkable ability to adapt to new defense measures.

The EDR wiping functionality gives the tool an edge over defenders responding to attacks but could also provide new opportunities for detecting the attacks in the pre-encryption phase.

Source: https://www.bleepingcomputer.com/news/security/poortry-windows-driver-evolves-into-a-full-featured-edr-wiper/