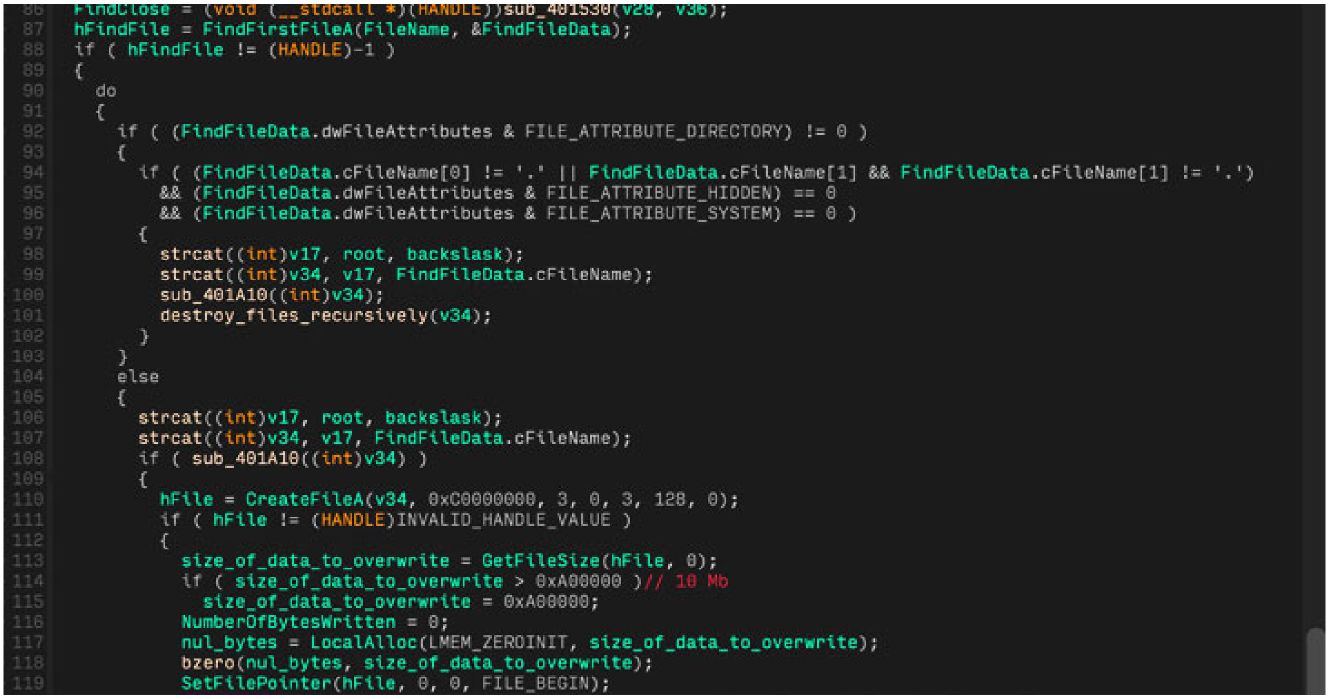
CaddyWiper: Yet Another Data Wiping Malware Targeting Ukrainian Networks

thehackernews.com/2022/03/caddywiper-yet-another-data-wiping.html

March 15, 2022



```
FindClose = (void (__stdcall *)(HANDLE))sub_401530(v28, v36);
hFindFile = FindFirstFileA(FileName, &FindFileData);
if ( hFindFile != (HANDLE)-1 )
{
  do
  {
    if ( (FindFileData.dwFileAttributes & FILE_ATTRIBUTE_DIRECTORY) != 0 )
    {
      if ( (FindFileData.cFileName[0] != '.' || FindFileData.cFileName[1] && FindFileData.cFileName[1] != '.')
        && (FindFileData.dwFileAttributes & FILE_ATTRIBUTE_HIDDEN) == 0
        && (FindFileData.dwFileAttributes & FILE_ATTRIBUTE_SYSTEM) == 0 )
      {
        strcat((int)v17, root, backslask);
        strcat((int)v34, v17, FindFileData.cFileName);
        sub_401A10((int)v34);
        destroy_files_recursively(v34);
      }
    }
    else
    {
      strcat((int)v17, root, backslask);
      strcat((int)v34, v17, FindFileData.cFileName);
      if ( sub_401A10((int)v34) )
      {
        hFile = CreateFileA(v34, 0xC0000000, 3, 0, 3, 128, 0);
        if ( hFile != (HANDLE)INVALID_HANDLE_VALUE )
        {
          size_of_data_to_overwrite = GetFileSize(hFile, 0);
          if ( size_of_data_to_overwrite > 0xA00000 )// 10 Mb
            size_of_data_to_overwrite = 0xA00000;
          NumberOfBytesWritten = 0;
          nul_bytes = LocalAlloc(LMEM_ZEROINIT, size_of_data_to_overwrite);
          bzero(nul_bytes, size_of_data_to_overwrite);
          SetFilePointer(hFile, 0, 0, FILE_BEGIN);
```

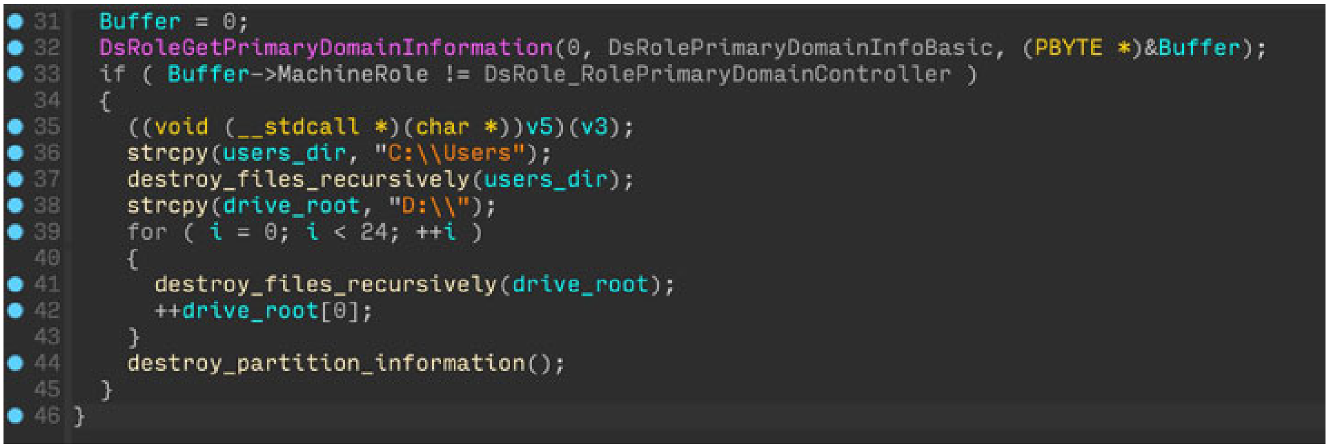
Two weeks after details emerged about a second data wiper strain delivered in attacks against Ukraine, yet another destructive malware has been detected amid Russia's continuing military invasion of the country.

Slovak cybersecurity company ESET dubbed the third wiper "**CaddyWiper**," which it said it first observed on March 14 around 9:38 a.m. UTC. Metadata associated with the executable ("caddy.exe") shows that the malware was compiled at 7:19 a.m. UTC, a little over two hours prior to its deployment.

CaddyWiper is notable for the fact that it doesn't share any similarities with previously discovered wipers in Ukraine, including HermeticWiper (aka FoxBlade or KillDisk) and IsaacWiper (aka Lasainraw), the two of which have been deployed in systems belonging to government and commercial entities.

"The ultimate goal of the attackers is the same as with IsaacWiper and HermeticWiper: make the systems unusable by erasing user data and partition information," Jean-Ian Boutin¸ head of threat research at ESET, told The Hacker News. "All of the organizations targeted by the recent wiper attacks were either in the governmental or financial sector."

Unlike CaddyWiper, both the HermeticWiper and IsaacWiper malware families are said to have been in development for months in advance before their release, with oldest known samples compiled on December 28 and October 19, 2021, respectively.



```
  Buffer = 0;
  DsRoleGetPrimaryDomainInformation(0, DsRolePrimaryDomainInfoBasic, (PBYTE *)&Buffer);
  if ( Buffer->MachineRole != DsRole_RolePrimaryDomainController )
  {
    ((void (__stdcall *)(char *))v5)(v3);
    strcpy(users_dir, "C:\\Users");
    destroy_files_recursively(users_dir);
    strcpy(drive_root, "D:\\");
    for ( i = 0; i < 24; ++i )
    {
      destroy_files_recursively(drive_root);
      ++drive_root[0];
    }
    destroy_partition_information();
  }
}
```

But the newly discovered wiper shares one tactical overlap with HermeticWiper in that the malware, in one instance, was deployed via the Windows domain controller, indicating that the attackers had taken control of the Active Directory server.

"Interestingly, CaddyWiper avoids destroying data on domain controllers," the company said. "This is probably a way for the attackers to keep their access inside the organization while still disturbing operations."

The wiper is programmed to systematically destroy all files located in "C:\Users," before moving on to the next drive letter and erasing the files until it reaches the "Z" drive, meaning CaddyWiper will also attempt to wipe any network mapped drive attached to the system.

"The file destruction algorithm is composed of two stages: a first stage to overwrite files and another to destroy the physical disk layout and the partition tables along with it," Cisco Talos researchers said in an analysis of the malware. "Destroying the start of the files and the partitions tables is a common technique seen on other wipers, and its highly effective in preventing file recovery."

Microsoft, which has attributed the HermeticWiper attacks to a threat cluster tracked as DEV-0665, said the "intended objective of these attacks is the disruption, degradation, and destruction of targeted resources" in the country.

The development also arrives as cybercriminals have opportunistically and increasingly capitalized on the conflict to design phishing lures, including themes of humanitarian assistance and various types of fundraising, to deliver a variety of backdoors such as Remcos.

"The global interest in the ongoing war in Ukraine makes it a convenient and effective news event for cybercriminals to exploit," Cisco Talos researchers said. "If a certain topic of lure is going to increase the chances of a potential victim installing their payload, they will use it."

But it's not just Ukraine that's been at the receiving end of wiper attacks. Last week, cybersecurity firm Trend Micro disclosed details of a .NET-based wiper called RURansom that has exclusively targeted entities in Russia by encrypting the files with a randomly generated cryptographic key.

"The keys are unique for each encrypted file and are not stored anywhere, making the encryption irreversible and marking the malware as a wiper rather than a ransomware variant," the researchers noted.

SHARE □ □ □ □ ךָ
SHARE □