SporaVaccination

github.com/MinervaLabsResearch/SporaVaccination

MinervaLabsResearch

MinervaLabsResearch/
SporaVaccination

Vaccinating against Spora ransomware: a proof-of-concept tool by Minerva

1 Contributor 0 Issues 1 Star 1 Fork

Vaccinating against Spora ransomware: a proof-of-concept tool by Minerva

Synopsis

Spora is presently among the most common ransomware families. For instance, it struck countless victims in the fake "Chrome Font Pack Update" campaign, encrypting victims' files even without having to communicate over the Internet. Minerva is releasing a proof-of-concept tool that is able to contain Spora infections by generating an infection marker that this ransomware seeks, to determine whether it's already running on the system.

This is a proof of concept demonstrating how to vaccinate against Spora. For more information, visit the following blog post: http://www.minerva-labs.com/post/vaccinating-against-spora-ransomware-a-proof-of-concept-tool-by-minerva

The code

The actual vaccination code can be found in the `VaccinateSpora()` method in `Program.cs`:

```
private bool VaccinateSpora()
{
    uint volumeSerialNumber, maxComponentLength;
    WinApi.FileSystemFeature fileSystemFlags;
    if (!WinApi.GetVolumeInformation(@"C:\", null, 0, out volumeSerialNumber, out
maxComponentLength, out fileSystemFlags, null, 0))
    {
        return false;
    }

    string mutexName = "m" + volumeSerialNumber;
    if (WinApi.CreateMutex(IntPtr.Zero, false, mutexName) == IntPtr.Zero)
    {
        return false;
    }

    return true;
}
```