**Harmon.ie**

February 11th, 2019.

**Description**

This is a review of Harmon.ie[[1]](#footnote-1) which identifies vulnerabilities related to windows registry, security settings, and network connections.

Adversaries could use a combination of these vulnerabilities to obtain unauthorized access through information gathering (discovery) techniques and mechanisms to bypass user account controls.

The main components reviewed included dynamic link libraries (DLL) and executable files (EXE). The findings show vulnerabilities related to the use of deprecated libraries, suspicious files, executable installer (compiler), and required privilege to install the software.

**Summary**

[General Aspects 2](#_Toc780707)

[Red Flags 5](#_Toc780708)

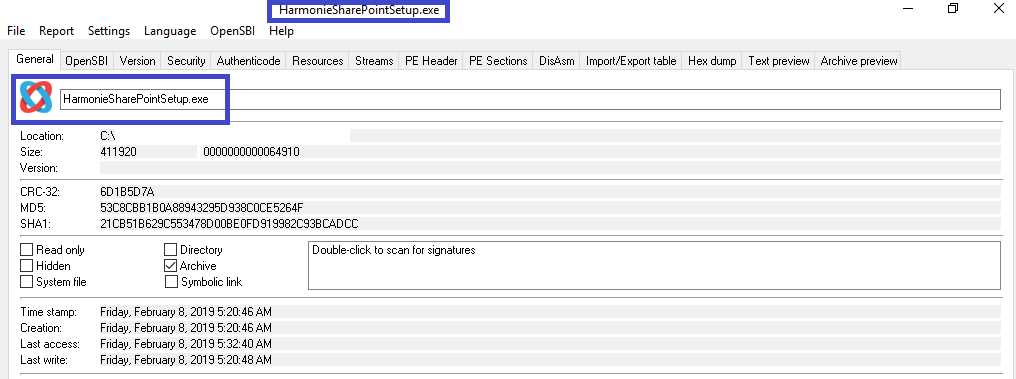
[Registry 5](#_Toc780709)

[Key components 7](#_Toc780710)

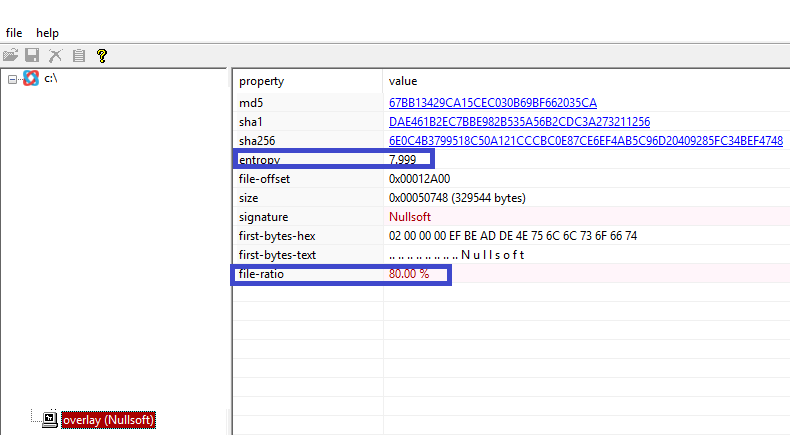
[Risk Assessment 10](#_Toc780711)

# General Aspects

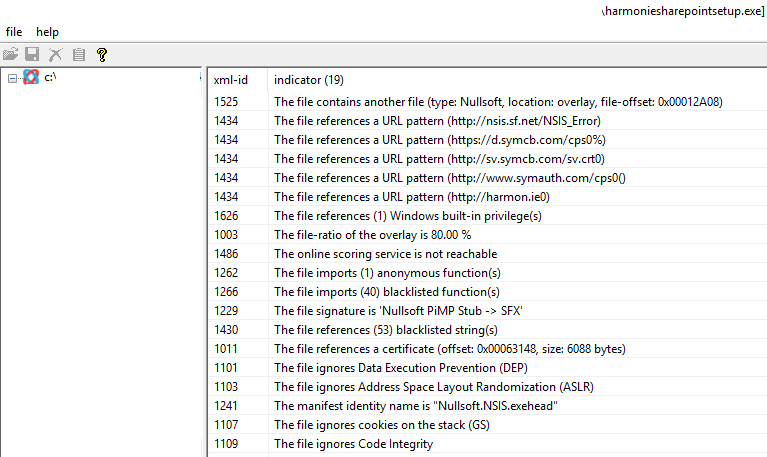
1. File identification



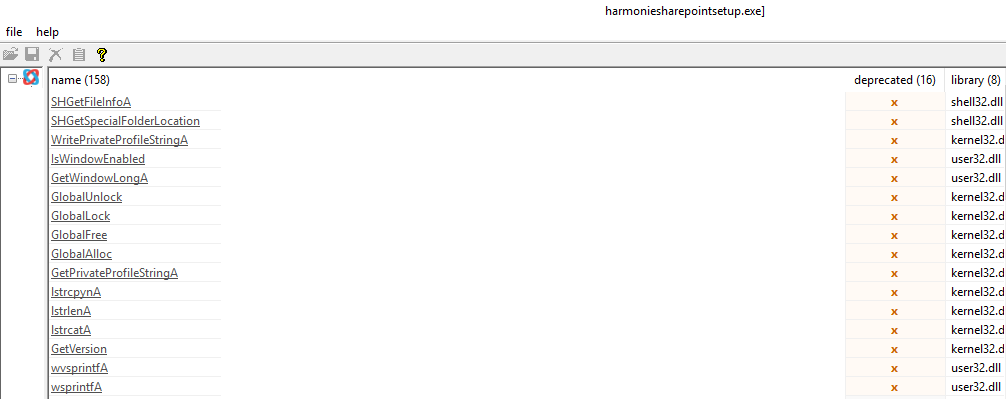
1. There is a high level of entropy and file-ratio.

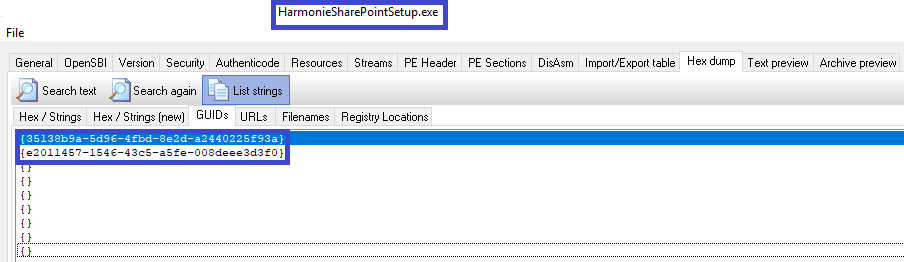


1. Initial diagnostic shows that:

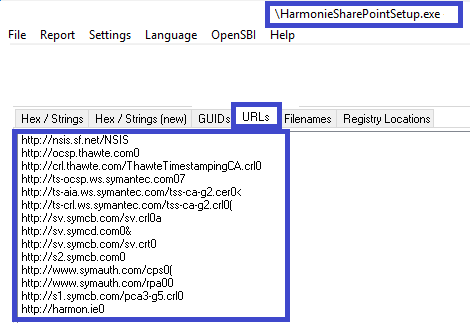


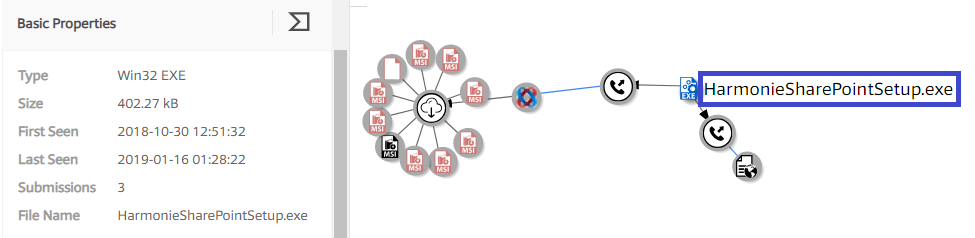
1. These are deprecated functions that could be related to the use associated with old Windows versions[[2]](#footnote-2):



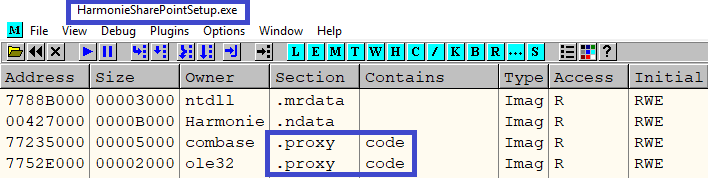
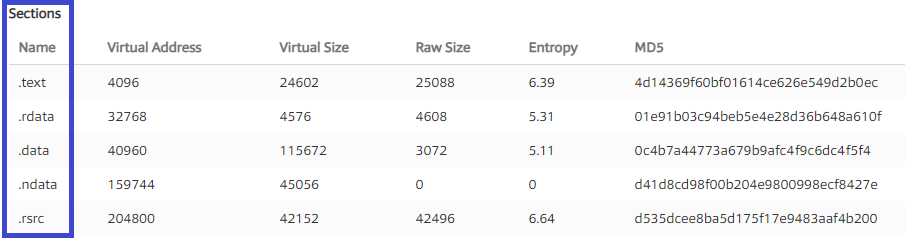


1. The software creates access to suspicious websites as we can see below[[3]](#footnote-3):





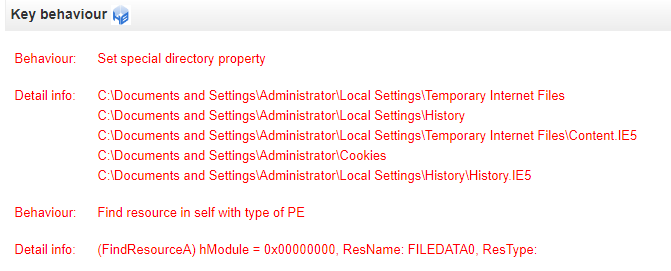
1. The software creates new sections with additional code:



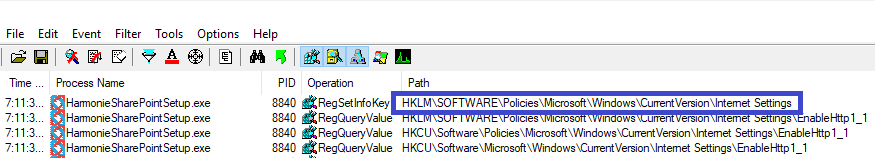
# Red Flags

## Registry

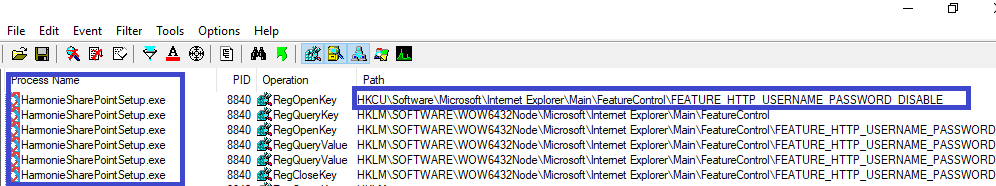
The software has unusual behaviours:



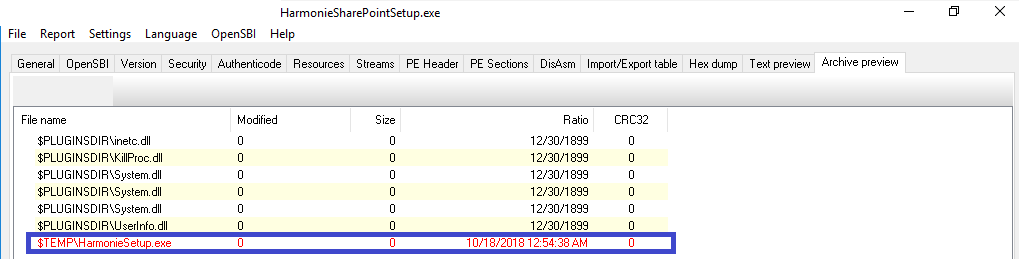
We can see that it queries the internet settings:



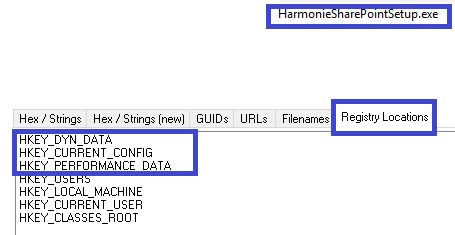
Check users and passwords[[4]](#footnote-4) settings:

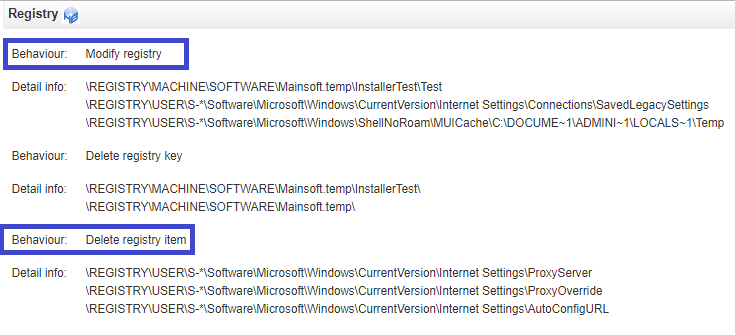


The software copies itself in a temporary file[[5]](#footnote-5):



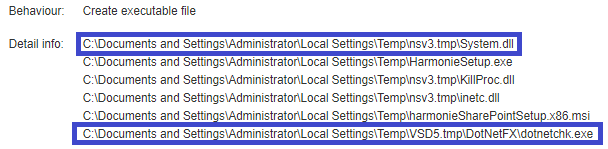
The software can collect, modify and delete information in the registry[[6]](#footnote-6):

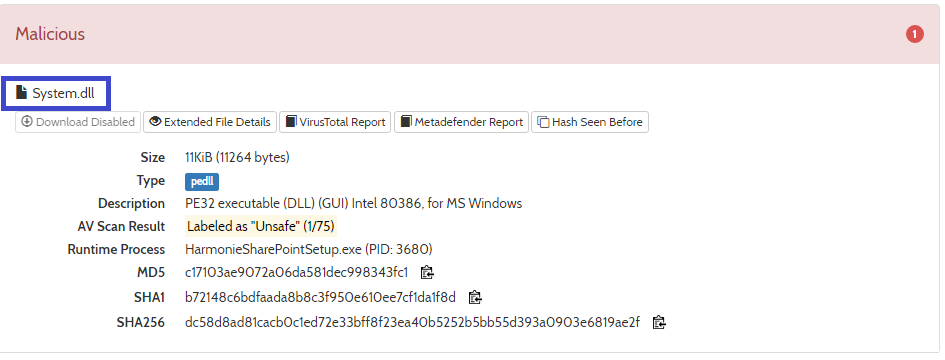


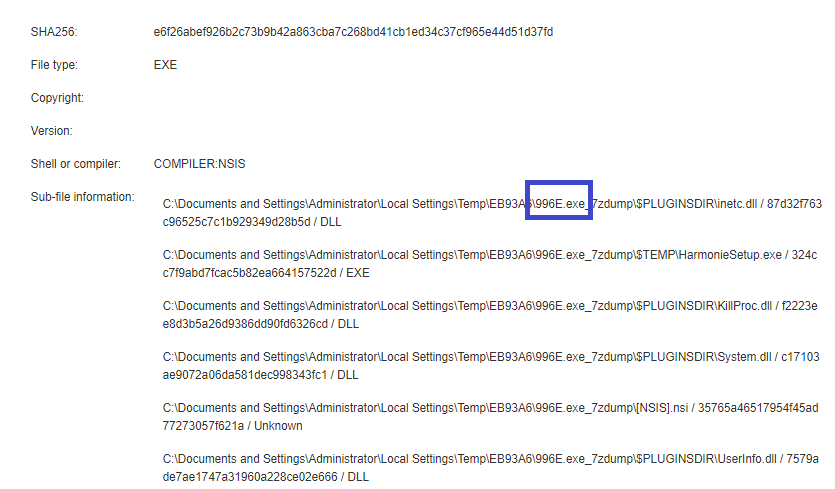


## Key components

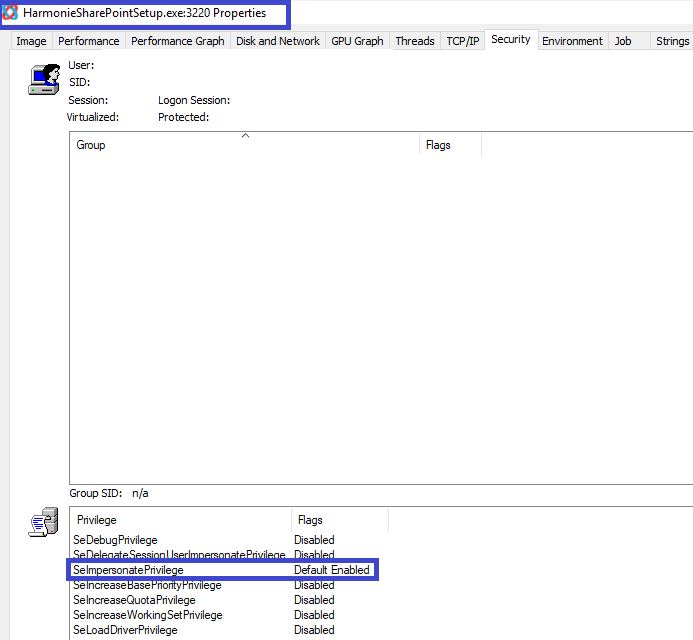
The software introduces a few unsecure components such as System.dll, dotnechk.exe[[7]](#footnote-7) and possibly the 996E.exe[[8]](#footnote-8).



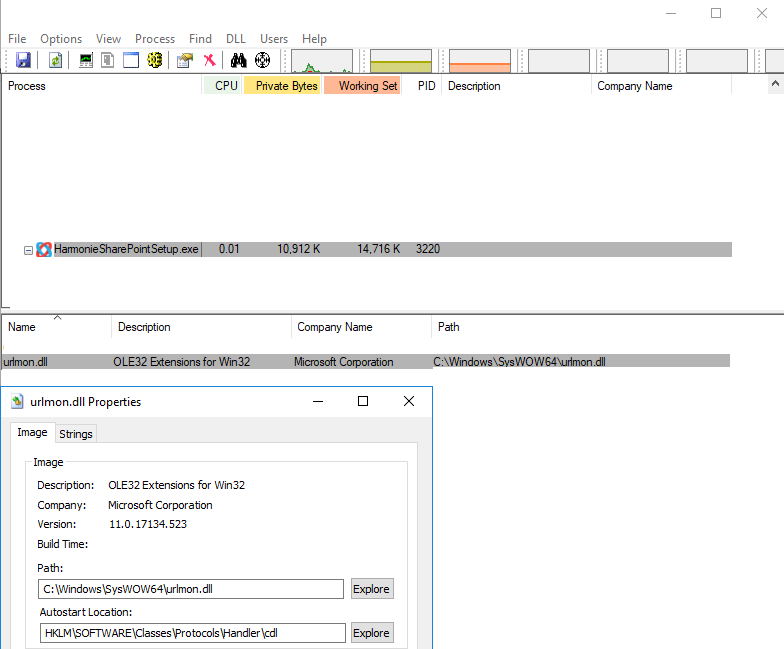




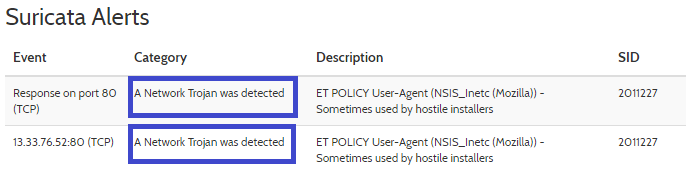
There is the risk of privilege escalation[[9]](#footnote-9)

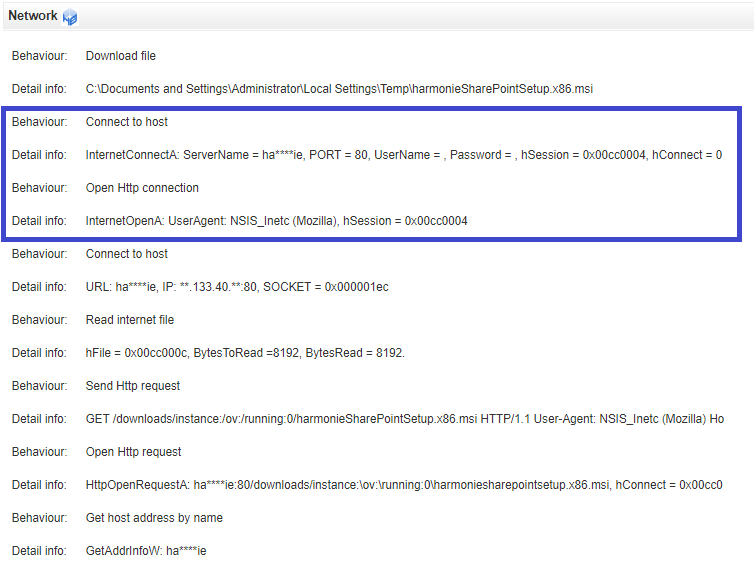


There is the use of an unsecure \*.dll (e.g. urlmon.dll[[10]](#footnote-10))



Suspicious alerts were identified in relation to the network access.

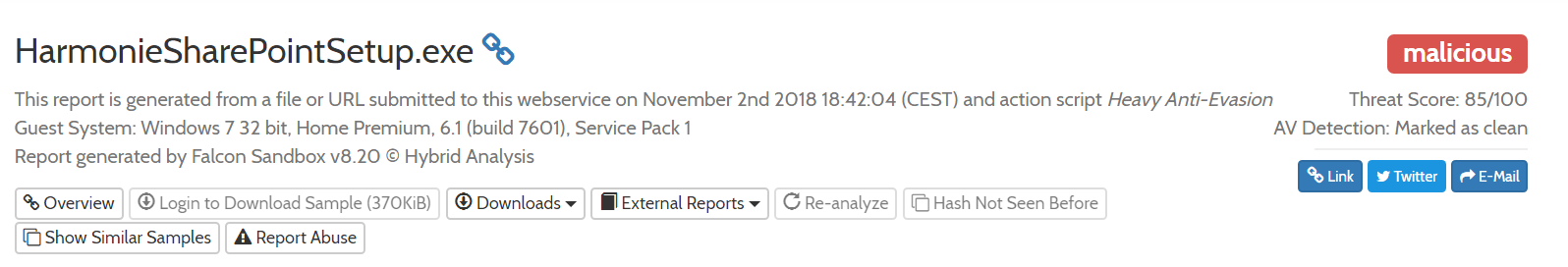


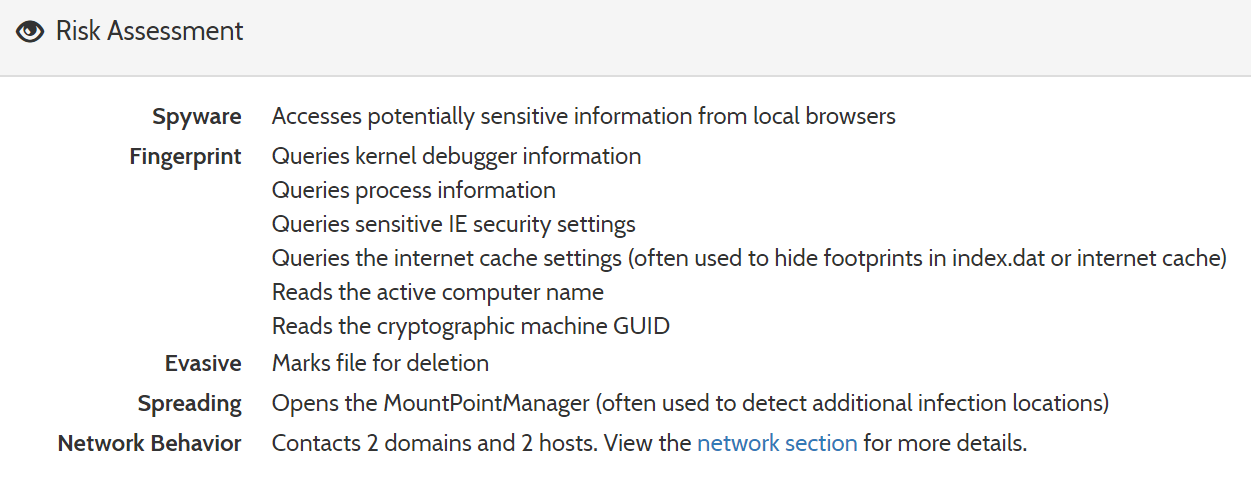


A possible explanation for vulnerabilities in the network and escalation privilege could be related to the Nullsoft Scriptable Install System (NSIS) component[[11]](#footnote-11) in use in this software[[12]](#footnote-12).

# Risk Assessment

The antivirus behaviour analysis shows a malicious result[[13]](#footnote-13):





1. https://harmon.ie/ [↑](#footnote-ref-1)
2. <https://docs.microsoft.com/en-us/windows/desktop/win7appqual/compatibility---application-manifest> [↑](#footnote-ref-2)
3. <https://www.virustotal.com/#/file/e6f26abef926b2c73b9b42a863cba7c268bd41cb1ed34c37cf965e44d51d37fd/details> [↑](#footnote-ref-3)
4. <https://support.microsoft.com/en-ca/help/834489/internet-explorer-does-not-support-user-names-and-passwords-in-web-sit> [↑](#footnote-ref-4)
5. <https://www.rsa.com/en-us/blog/2017-04/why-malware-installers-use-tmp-files-and-the-temp-folder> [↑](#footnote-ref-5)
6. <https://docs.microsoft.com/en-us/dotnet/api/microsoft.win32.registry.dyndata?view=netframework-4.7.2> [↑](#footnote-ref-6)
7. <https://file-intelligence.comodo.com/windows-process-virus-malware/exe/dotnetchk> [↑](#footnote-ref-7)
8. <https://www.exefilesupport.com/easy-guide-to-remove-996e-exe-from-pc> [↑](#footnote-ref-8)
9. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication> [↑](#footnote-ref-9)
10. <https://file-intelligence.comodo.com/windows-process-virus-malware/DLL/URLMON> [↑](#footnote-ref-10)
11. <https://www.cvedetails.com/cve/CVE-2015-0941/> [↑](#footnote-ref-11)
12. <https://seclists.org/fulldisclosure/2015/Dec/32> [↑](#footnote-ref-12)
13. <https://www.hybrid-analysis.com/sample/e6f26abef926b2c73b9b42a863cba7c268bd41cb1ed34c37cf965e44d51d37fd> [↑](#footnote-ref-13)