

Harmon.ie

February 11th, 2019.

Description

This is a review of Harmon.ie¹ 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.

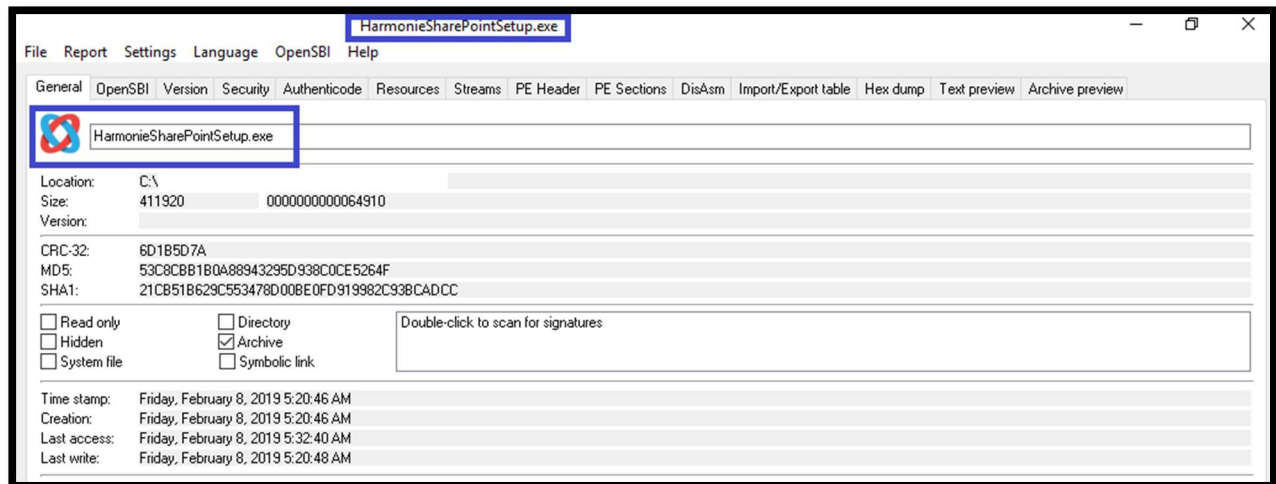
Summary

General Aspects	2
Red Flags.....	5
Registry	5
Key components.....	7
Risk Assessment	10

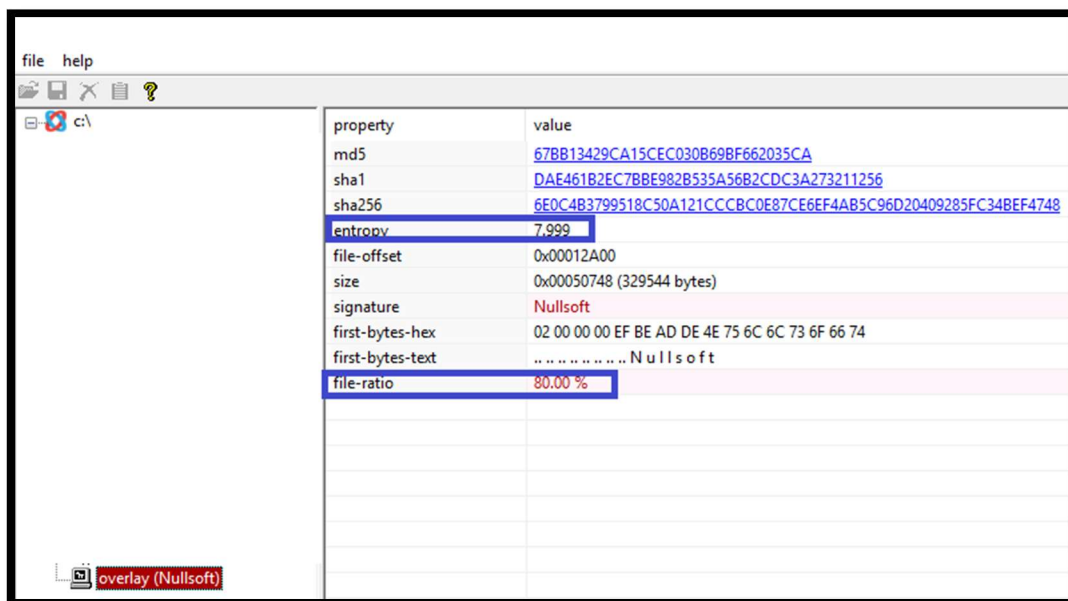
¹ <https://harmon.ie/>

General Aspects

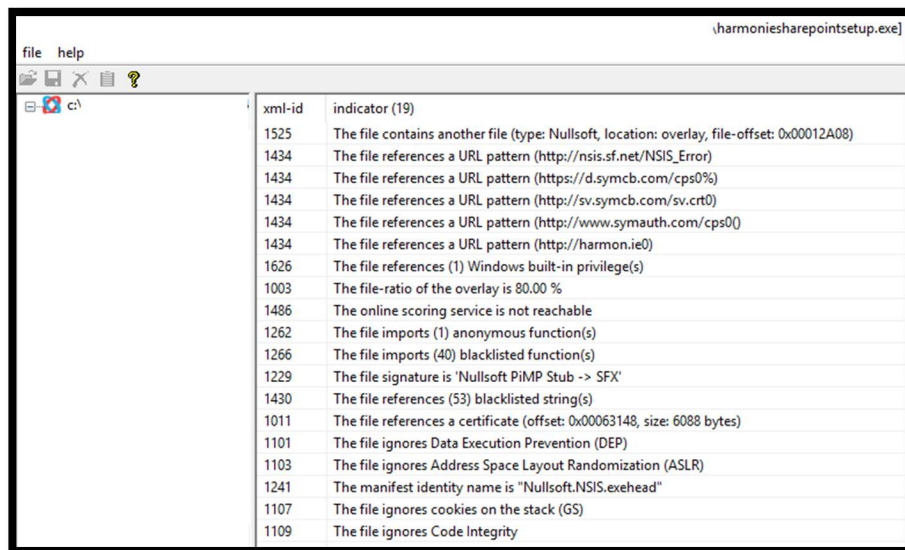
1. File identification



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

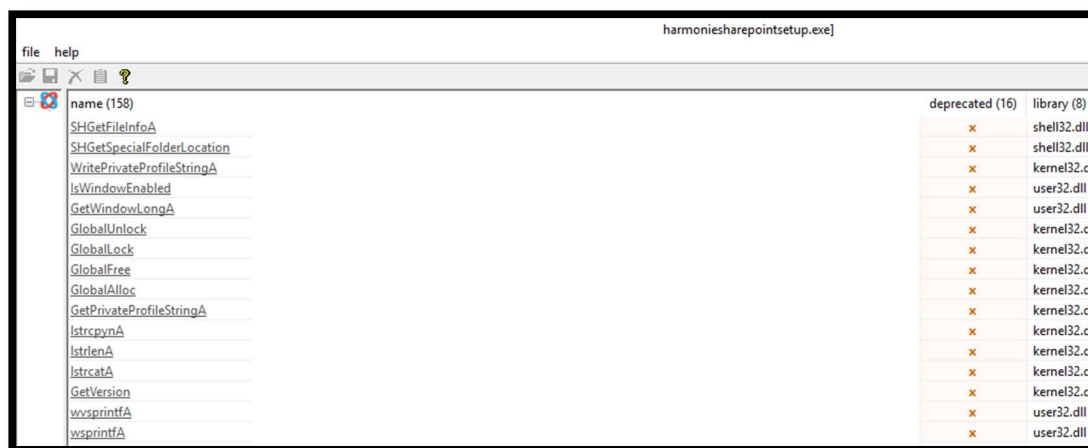


3. Initial diagnostic shows that:

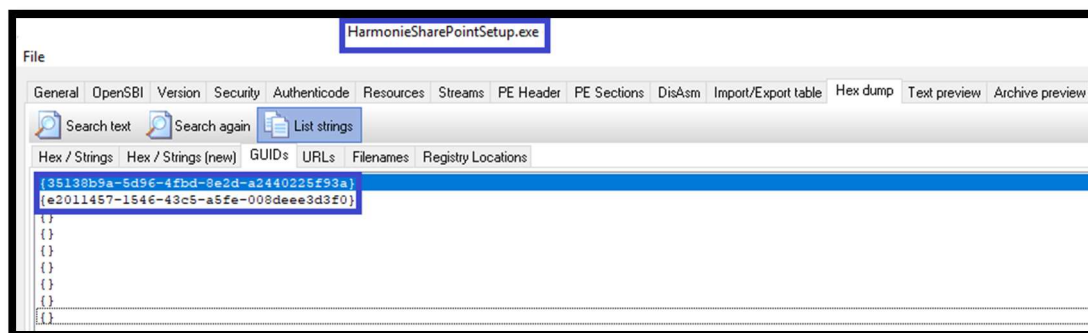


xml-id	indicator (19)
1525	The file contains another file (type: Nullsoft, location: overlay, file-offset: 0x00012A08)
1434	The file references a URL pattern (http://nsis.sf.net/NSIS_Error)
1434	The file references a URL pattern (https://d.symcb.com/cps0%)
1434	The file references a URL pattern (http://sv.symcb.com/sv.crt0)
1434	The file references a URL pattern (http://www.symauth.com/cps0)
1434	The file references a URL pattern (http://harmon.ie0)
1626	The file references (1) Windows built-in privilege(s)
1003	The file-ratio of the overlay is 80.00 %
1486	The online scoring service is not reachable
1262	The file imports (1) anonymous function(s)
1266	The file imports (40) blacklisted function(s)
1229	The file signature is 'Nullsoft PiMP Stub -> SFX'
1430	The file references (53) blacklisted string(s)
1011	The file references a certificate (offset: 0x00063148, size: 6088 bytes)
1101	The file ignores Data Execution Prevention (DEP)
1103	The file ignores Address Space Layout Randomization (ASLR)
1241	The manifest identity name is "Nullsoft.NSIS.exehead"
1107	The file ignores cookies on the stack (GS)
1109	The file ignores Code Integrity

4. These are deprecated functions that could be related to the use associated with old Windows versions²:



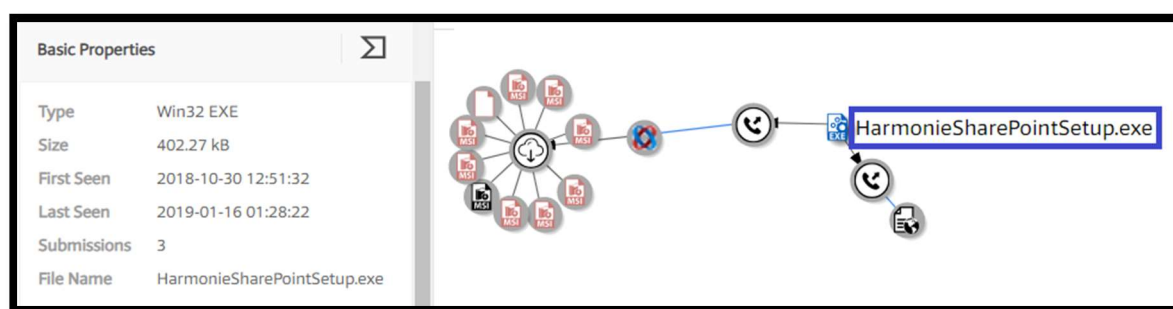
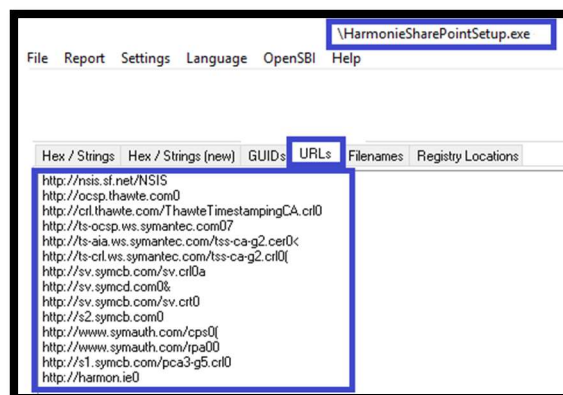
name (158)	deprecated (16)	library (8)
SHGetFileInfoA	x	shell32.dll
SHGetSpecialFolderLocation	x	shell32.dll
WritePrivateProfileStringA	x	kernel32.d
IsWindowEnabled	x	user32.dll
GetWindowLongA	x	user32.dll
GlobalUnlock	x	kernel32.d
GlobalLock	x	kernel32.d
GlobalFree	x	kernel32.d
GlobalAlloc	x	kernel32.d
GetPrivateProfileStringA	x	kernel32.d
lstrcpynA	x	kernel32.d
lstrlenA	x	kernel32.d
lstrcatA	x	kernel32.d
GetVersion	x	kernel32.d
wsprintfA	x	user32.dll
wsprintfA	x	user32.dll



File
HarmonieSharePointSetup.exe
General OpenSBI Version Security Authenticode Resources Streams PE Header PE Sections DisAsm Import/Export table Hex dump Text preview Archive preview
Search text Search again List strings
Hex / Strings Hex / Strings (new) GUIDs URLs Filenames Registry Locations
{35138b9a-5d96-4fbd-8e2d-a2440225f93a}
{e2011457-1546-43c5-a5fe-008deee3d3f0}
{ }
{ }
{ }
{ }
{ }
{ }

² <https://docs.microsoft.com/en-us/windows/desktop/win7appqual/compatibility---application-manifest>

5. The software creates access to suspicious websites as we can see below³:



6. The software creates new sections with additional code:

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	24602	25088	6.39	4d14369f60bf01614ce626e549d2b0ec
.rdata	32768	4576	4608	5.31	01e91b03c94beb5e4e28d36b648a610f
.data	40960	115672	3072	5.11	0c4b7a44773a679b9afc4f9c6dc4f5f4
.ndata	159744	45056	0	0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	204800	42152	42496	6.64	d535dcee8ba5d175f17e9483aaf4b200

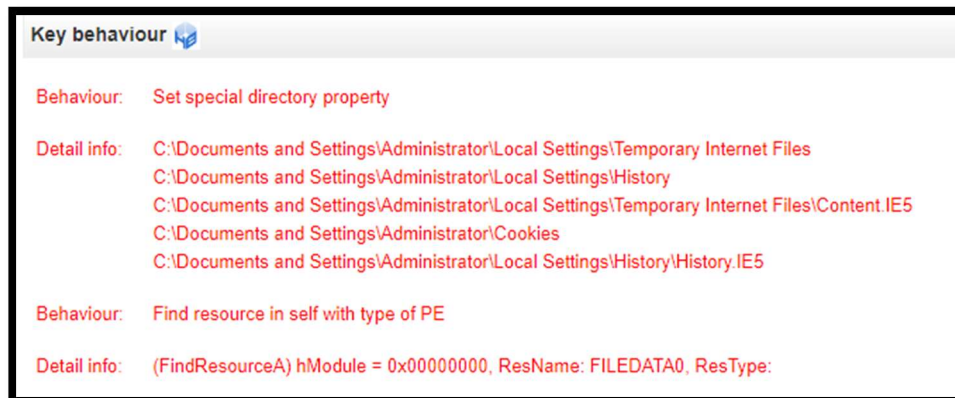
Address	Size	Owner	Section	Contains	Type	Access	Initial
7788B000	00003000	ntdll	.mrdata		Image	R	RWE
00427000	0000B000	Harmonie	.ndata		Image	R	RWE
77235000	00005000	combase	.proxy	code	Image	R	RWE
7752E000	00002000	ole32	.proxy	code	Image	R	RWE

³<https://www.virustotal.com/#/file/e6f26abef926b2c73b9b42a863cba7c268bd41cb1ed34c37cf965e44d51d37fd/details>

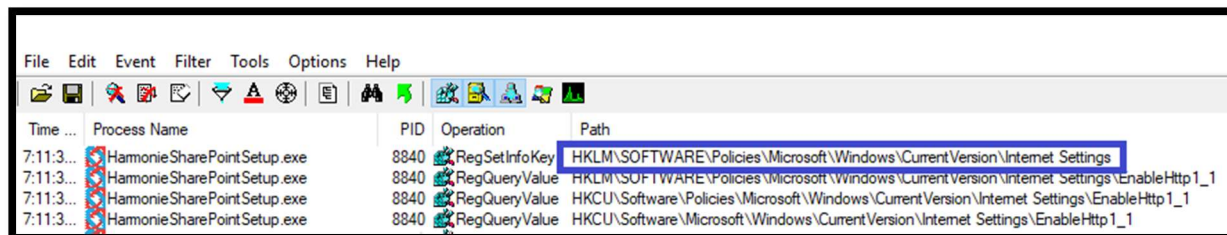
Red Flags

Registry

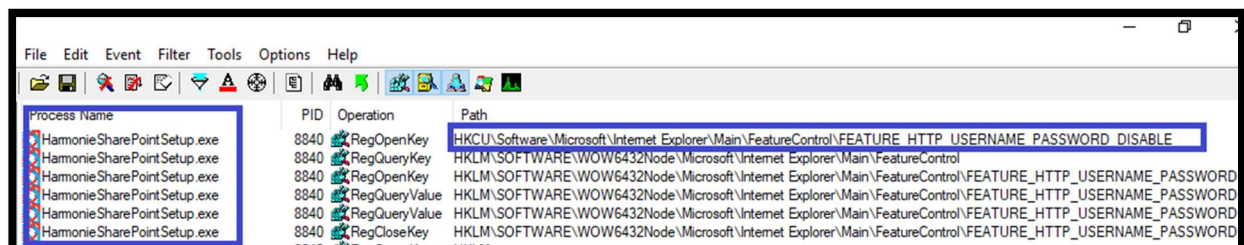
The software has unusual behaviours:



We can see that it queries the internet settings:

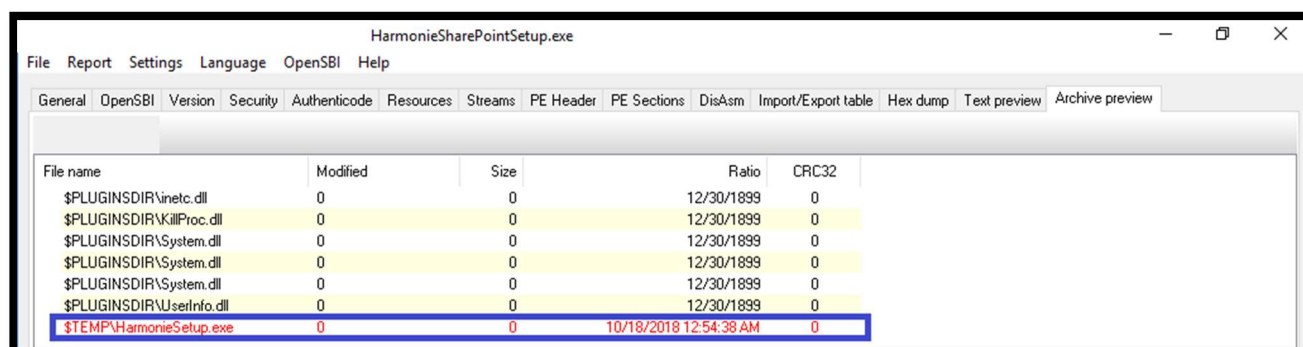


Check users and passwords⁴ settings:

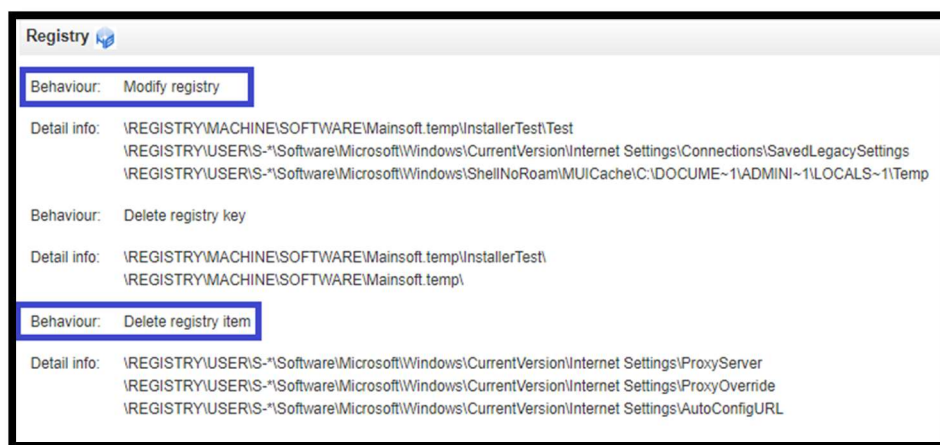
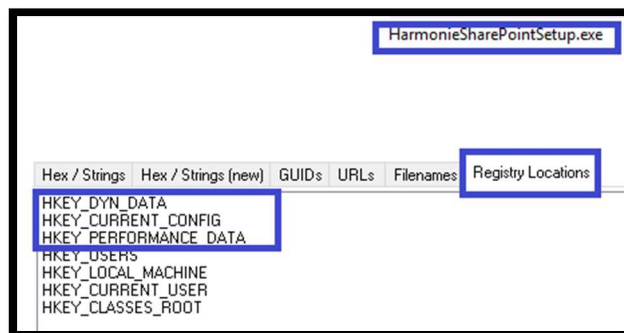


⁴ <https://support.microsoft.com/en-ca/help/834489/internet-explorer-does-not-support-user-names-and-passwords-in-web-sit>

The software copies itself in a temporary file⁵:



The software can collect, modify and delete information in the registry⁶:

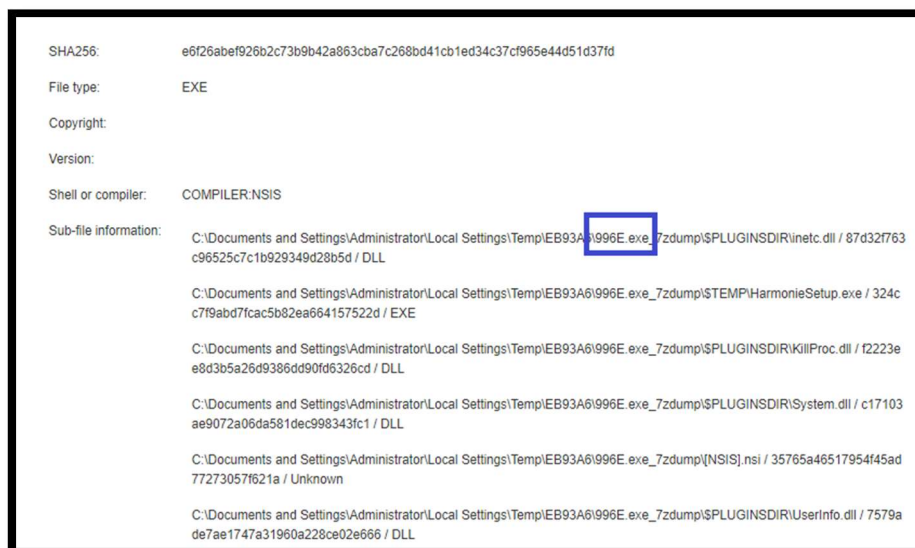
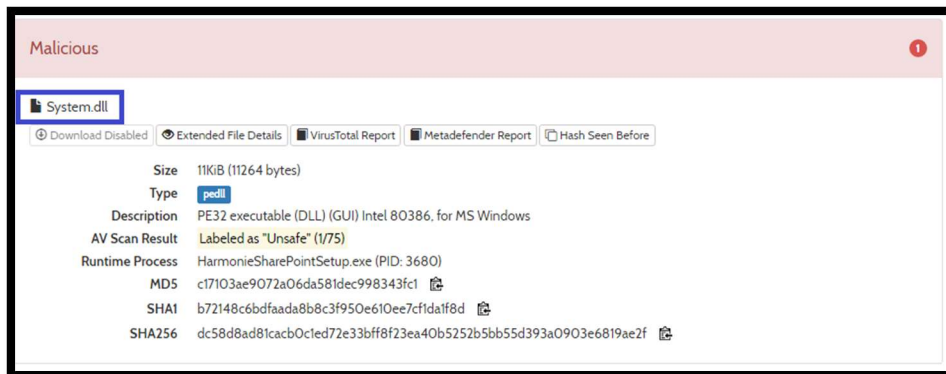
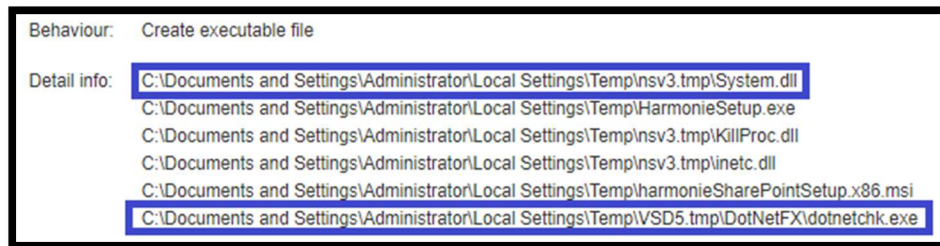


⁵ <https://www.rsa.com/en-us/blog/2017-04/why-malware-installers-use-tmp-files-and-the-temp-folder>

⁶ <https://docs.microsoft.com/en-us/dotnet/api/microsoft.win32.registry.dyndata?view=netframework-4.7.2>

Key components

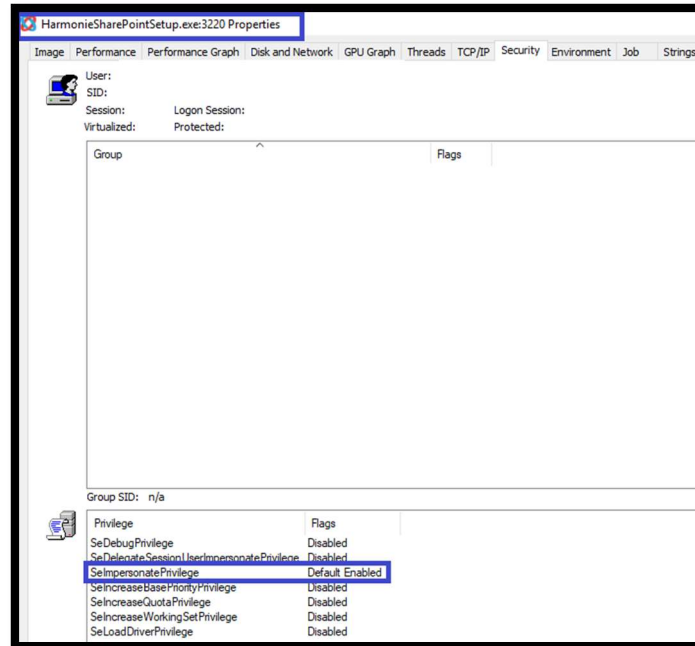
The software introduces a few unsecure components such as System.dll, dotnechk.exe⁷ and possibly the 996E.exe⁸.



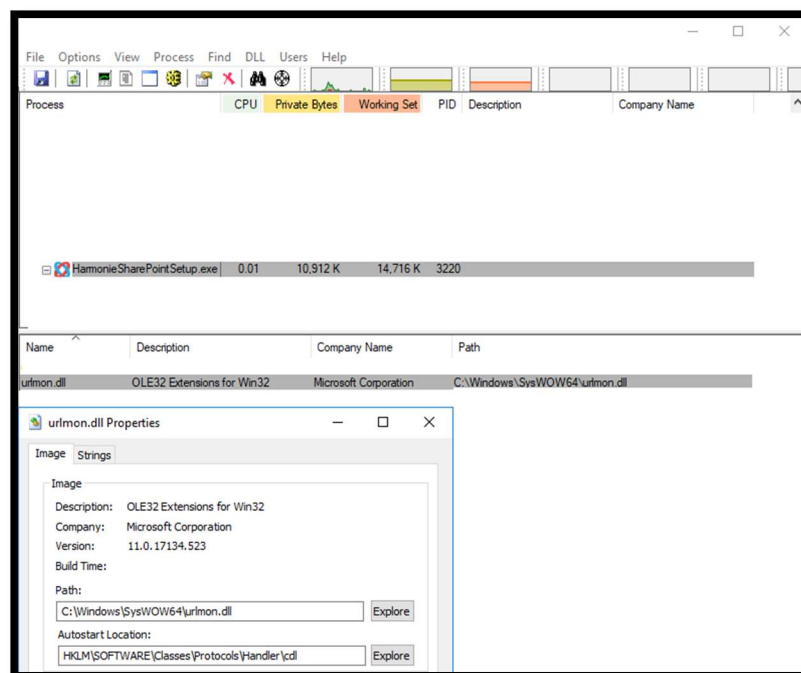
⁷ <https://file-intelligence.comodo.com/windows-process-virus-malware/exe/dotnetchk>

⁸ <https://www.exfilesupport.com/easy-guide-to-remove-996e-exe-from-pc>

There is the risk of privilege escalation⁹



There is the use of an unsecure *.dll (e.g. urlmon.dll¹⁰)



⁹ <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication>

¹⁰ <https://file-intelligence.comodo.com/windows-process-virus-malware/DLL/URLMON>

Suspicious alerts were identified in relation to the network access.

Suricata Alerts			
Event	Category	Description	SID
Response on port 80 (TCP)	A Network Trojan was detected	ET POLICY User-Agent (NSIS_Inetc (Mozilla)) - Sometimes used by hostile installers	2011227
13.33.76.52:80 (TCP)	A Network Trojan was detected	ET POLICY User-Agent (NSIS_Inetc (Mozilla)) - Sometimes used by hostile installers	2011227

Network	
Behaviour:	Download file
Detail info:	C:\Documents and Settings\Administrator\Local Settings\Temp\harmonieSharePointSetup.x86.msi
Behaviour:	Connect to host
Detail info:	InternetConnectA: ServerName = ha****ie, PORT = 80, UserName = , Password = , hSession = 0x00cc0004, hConnect = 0
Behaviour:	Open Http connection
Detail info:	InternetOpenA: UserAgent: NSIS_Inetc (Mozilla), hSession = 0x00cc0004
Behaviour:	Connect to host
Detail info:	URL: ha****ie, IP: *.133.40.**:80, SOCKET = 0x000001ec
Behaviour:	Read internet file
Detail info:	hFile = 0x00cc000c, BytesToRead = 8192, BytesRead = 8192.
Behaviour:	Send Http request
Detail info:	GET /downloads/instance:/ov:/running:0/harmonieSharePointSetup.x86.msi HTTP/1.1 User-Agent: NSIS_Inetc (Mozilla) Ho
Behaviour:	Open Http request
Detail info:	HttpOpenRequestA: ha****ie:80/downloads/instance:/ov:/running:0/harmoniesharepointsetup.x86.msi, hConnect = 0x00cc0
Behaviour:	Get host address by name
Detail info:	GetAddrInfoW: ha****ie

A possible explanation for vulnerabilities in the network and escalation privilege could be related to the Nullsoft Scriptable Install System (NSIS) component¹¹ in use in this software¹².

¹¹ <https://www.cvedetails.com/cve/CVE-2015-0941/>

¹² <https://seclists.org/fulldisclosure/2015/Dec/32>

Risk Assessment

The antivirus behaviour analysis shows a malicious result¹³:

HarmonieSharePointSetup.exe

malicious

This report is generated from a file or URL submitted to this webservice on November 2nd 2018 18:42:04 (CEST) and action script *Heavy Anti-Evasion* Threat Score: 85/100
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1 AV Detection: Marked as clean
Report generated by Falcon Sandbox v8.20 © Hybrid Analysis

[Overview](#) [Login to Download Sample \(370KiB\)](#) [Downloads](#) [External Reports](#) [Re-analyze](#) [Hash Not Seen Before](#)

[Show Similar Samples](#) [Report Abuse](#)

[Link](#) [Twitter](#) [E-Mail](#)

Risk Assessment

Spyware	Accesses potentially sensitive information from local browsers
Fingerprint	Queries kernel debugger information Queries process information Queries sensitive IE security settings Queries the internet cache settings (often used to hide footprints in index.dat or internet cache) Reads the active computer name Reads the cryptographic machine GUID
Evasive	Marks file for deletion
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior	Contacts 2 domains and 2 hosts. View the network section for more details.

¹³ <https://www.hybrid-analysis.com/sample/e6f26abef926b2c73b9b42a863cba7c268bd41cb1ed34c37cf965e44d51d37fd>