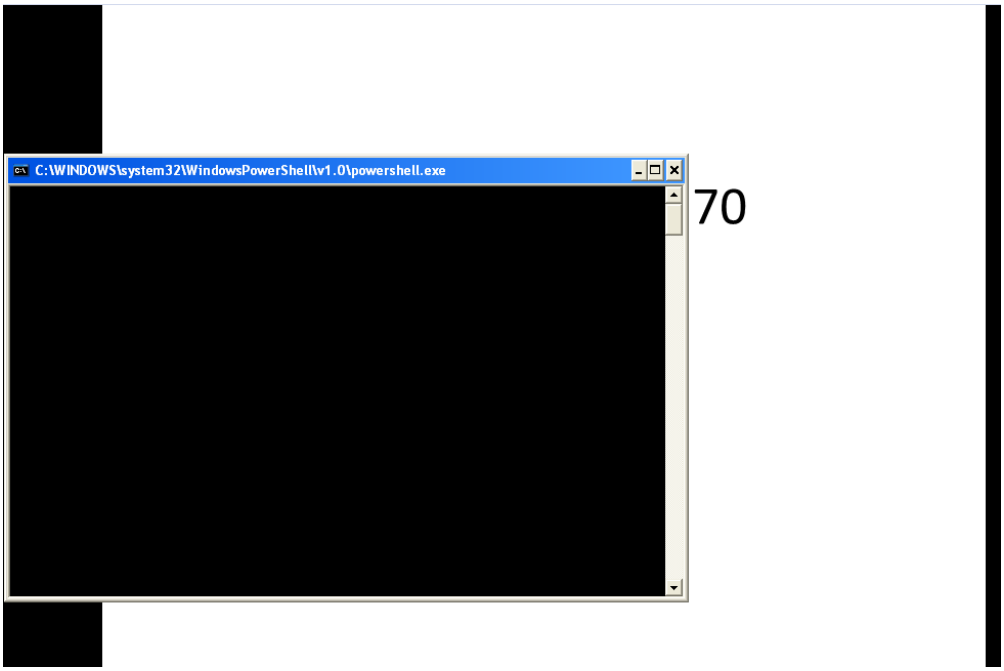
2017 7 Microsoft Office
CVE-2017-8570 2017 7
github CVE-2017-8570 7 29

CVE-2017-8570
SandWorm

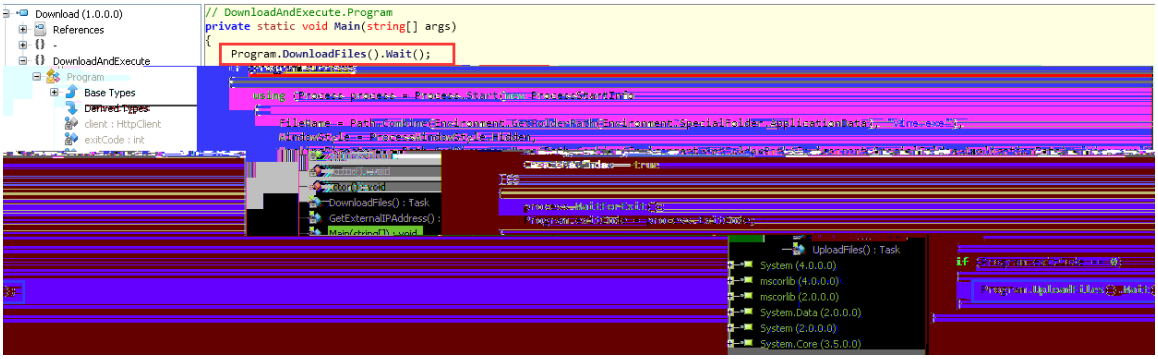
5

CVE-2017-8570

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)



5. powershell download.exe download.exe Vine.exe

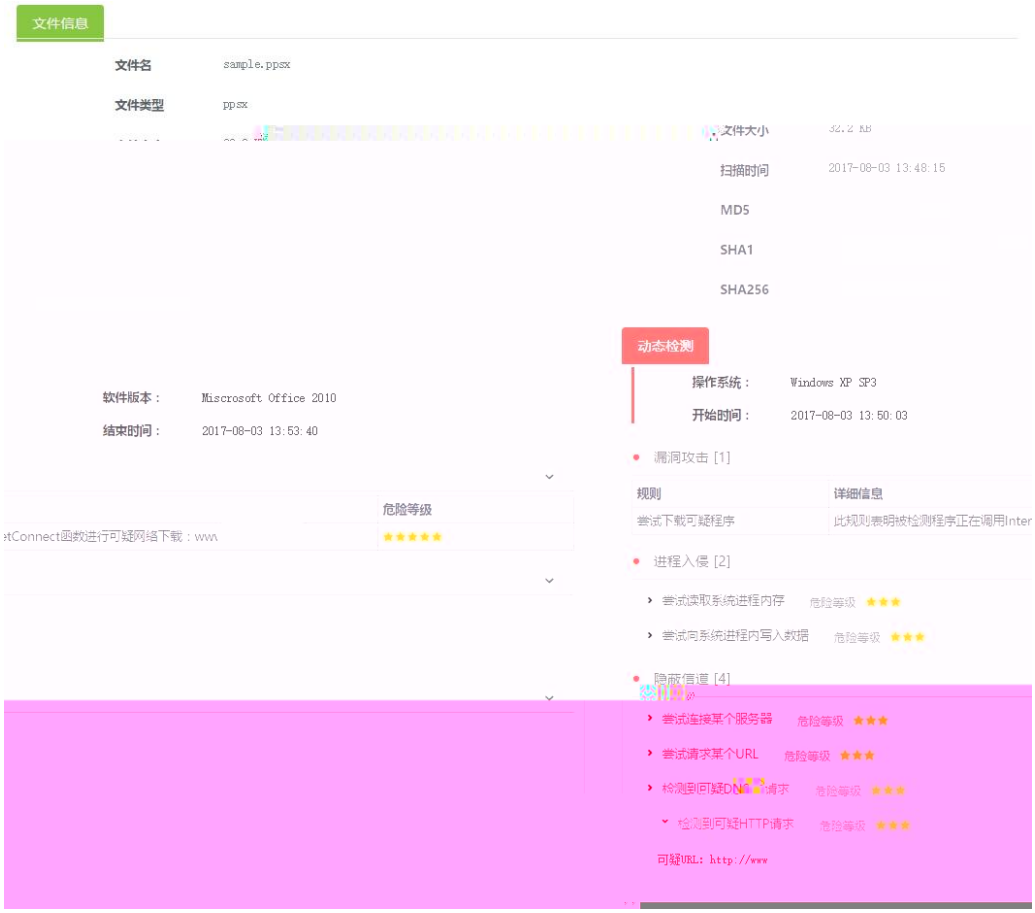


6. Vine.exe Chrome Firefox download.exe

1. 2017 7

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570

2.


文件信息
文件名
sample.ppsx
文件类型
ppsx
文件大小
32.2 KB
扫描时间
2017-08-03 13:48:15
MD5
SHA1
SHA256
动态检测
操作系统：
Windows XP SP3
开始时间：
2017-08-03 13:50:03
软件版本：
Miscrosoft Office 2010
结束时间：
2017-08-03 13:53:40
漏洞攻击 [1]
规则
详细信息
尝试下载可疑程序
此规则表明被检测程序正在调用Inter
危险等级
etConnect函数进行可疑网络下载：www
进程入侵 [2]
尝试读取系统进程内存
危险等级
尝试向系统进程内写入数据
危险等级
隐蔽信道 [4]
尝试连接某个服务器
危险等级
尝试请求某个URL
危险等级
检测到可疑DNS请求
危险等级
检测到可疑HTTP请求
危险等级
可疑URL: http://www