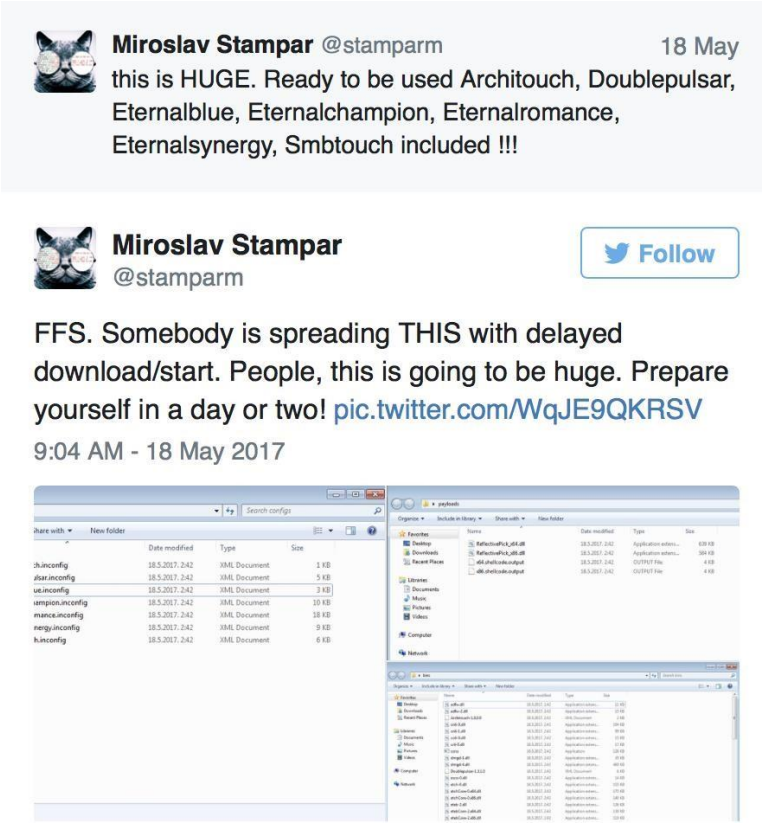
永恒之石 EternalRocks 蠕虫病毒处理建议

近期，安全研究人员发现了一款新的恶意软件。这款恶意软件与 WannaCry 勒索软件一样，通过利用 Windows SMB 文件共享协议中的漏洞自行传播，但是与后者不同的是，它使用了近期泄露的美国国家安全局（NSA）的多种黑客工具，该病毒除了会利用“永恒之蓝”漏洞发动攻击外，也会尝试 NSA 泄露的其他漏洞进行攻击。

病毒介绍

2017 年 5 月 17 日，克罗地亚安全专家（Miroslav Stampar）发现了一种基于类似 WannaCry 的蠕虫病毒，也是通过 NSA 武器库中的漏洞进行传播，他将此病毒命名为 EternalRocks， 据国外媒体《财富》杂志 2017 年 5 月 21 日报道，EternalRocks 影响了大量未安装补丁的 Windows7 主机，传播速度快，



Eternalrocks 由 7 个攻击载荷组成，包括 4 个 Windows 漏洞利用程序、1 个后门程序和 2 个漏洞扫描程序。

功能	模块名	漏洞编号

漏洞利用程序	Eternalblue Eternalchampion Eternalromance Eternalsynergy	Microsoft Windows SMB 远程代码执行漏洞(MS17-010) CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148
后门程序	Doublepulsar	
扫描程序	Architouch、Smbtouch	

上述提到的 4 个漏洞利用均利用了 Windows 系统 SMB 协议存在的漏洞，涉及 Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2 系统，微软已经发布官方安全补丁 MS17-010，对漏洞进行了修复。

病毒工作流程如下：

处理预防建议

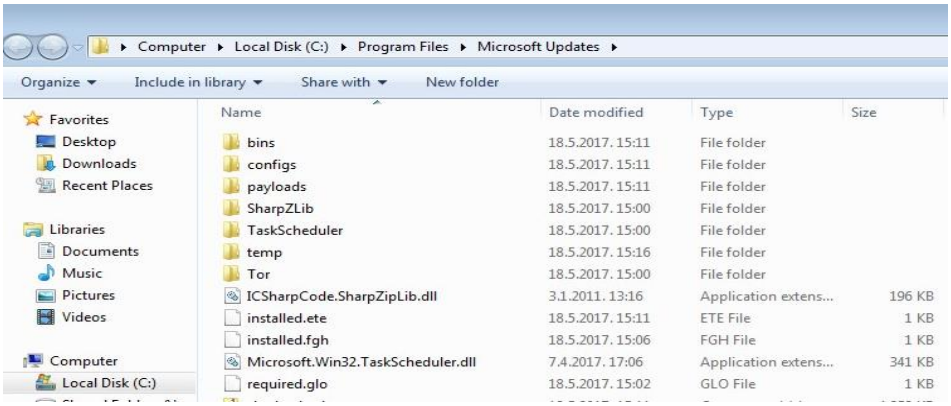
预防加固

- 确保安全更新补丁 MS17-010 已经在电脑上更新安装，并开启补丁更新功能；
- 建议打开系统防火墙并更新系统上反病毒软件，并确保病毒库的及时更新；
- 不随意使用盗版、破解版操作系统和 office 软件；
- 不轻易打开任何可疑的未知陌生的文档文件和邮件附件；

预防检测

1，确认是否存在以下多余文件夹

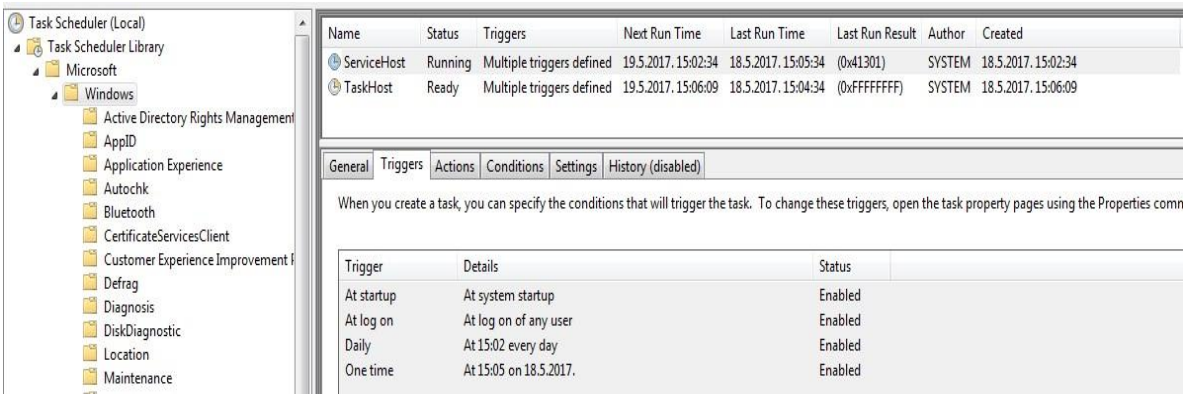
病毒感染主机后，会创建 C:\Program Files\Microsoft Updates\目录，生成多个病毒文件，如下图：



2，检查是否有相关计划任务

点击开始菜单——控制面板——管理工具——计划任务，展开任务计划程序库——Microsoft ——Windows，

病毒会创建 2 个计划任务 ServiceHost 和 TaskHost，如下图：



在主机上发现以上特征，即可判断已经感染 EternalRocks 病毒。

3，感染处理建议

- 如发现计算机已经感染病毒，立即断开网络等方式进行隔离，避免病毒进一步扩散；
- 进入开始菜单—控制面板—管理工具—计划任务，展开任务计划程序库—Microsoft—Windows，删除计划任务 ServiceHost 和 TaskHost；
- 停止以下进程

  C:\Program Files\Microsoft Updates\svchost.exe

  C:\Program Files\Microsoft Updates\taskhost.exe

  C:\Program Files\Microsoft Updates\torunzip.exe
- 删除 C:\Program Files\Microsoft Updates\目录及其中所有文件；
- 下载并安装系统上述相关安全补丁；
- 跟踪留意病毒是否依然存在，使用最新杀毒软件对系统进行全面完整扫描；