**驱动人生家族概述**

驱动人生家族的木马为无文件类型后门，具备自主横向传播的能力，未打永恒之蓝相关漏洞补丁的电脑容易成为攻击目标。同时，该木马还会结合口令爆破、弱密码、文件共享等手段横向传播。

**如何排查是否中招**

中招该家族，最典型的特点为：

1. Windows目录下出现大量随机文件名的恶意文件，并有大量服务指向这些随机文件:



1. 机器上存在攻击其他机器（横向传播）的行为。 下图中的ewhizou.exe（文件名随机）即在尝试攻击其他机器。



1. 大量powershell进程持续占用cpu资源（上图）进行挖矿，导致机器卡慢。

**处置建议**

由于驱动人生具备自主横向移动能力，因此同局域网下若还有一台机器存在该病毒，在防护不到位的情况下，依然会重复感染该病毒，其外在表现是：天擎出现反复查杀的行为，系统CPU持续高占用。

**处置步骤（不可遗漏、不可跳过）：**

1. 断网
2. 使用天擎进行全盘扫描并执行最终清理动作（需要确保所有清理动作完成而不是未处理或处理失败）
3. 再次确认windows服务项中不存在指向windows目录下随机文件名的服务
4. 重启系统
5. 给系统打上如下补丁（不同版本系统对应的补丁不同， 更详细信息参考本文最后）：
* KB4012598
* KB4012212
* KB4013429
* KB4013198
* KB4012606
1. 修改用户密码， 设置一个强壮密码（6位以上， 包含数字、字母、特殊符号），且不同机器之间的密码需要不一样。
2. 关闭不必要的共享目录
3. 重启系统
4. 恢复联网

**加固措施：**

定时更新病毒库

周期性执行全盘扫描

及时给系统打重要补丁

**补丁详细信息：**

**补丁地址：**

**Windows XP**
Windows XP SP3 安全更新程序 (KB4012598) 下载地址
https://www.microsoft.com/en-us/download/details.aspx?id=55245
Windows XP SP2 x64 （64位）安全更新程序 (KB4012598) 下载地址
http://www.microsoft.com/downloads/details.aspx?FamilyId=5fbaa61b-15ce-49c7-9361-cb5494f9d6aa

**Windows Server 2003**
Windows Server 2003 SP2 x86 安全更新程序 (KB4012598) 下载地址
https://www.microsoft.com/en-us/download/details.aspx?id=55248
Windows Server 2003 SP2 x64 （64位）安全更新程序 (KB4012598) 下载地址
https://www.microsoft.com/en-us/download/details.aspx?id=55244

**Windows 8**
Windows 8 x86 安全更新程序 (KB4012598) 下载地址
http://www.microsoft.com/downloads/details.aspx?FamilyId=6e2de6b7-9e43-4b42-aca2-267f24210340
Windows 8 x64 （64位）安全更新程序 (KB4012598) 下载地址
http://www.microsoft.com/downloads/details.aspx?FamilyId=b08bb3f1-f156-4e61-8a68-077963bae8c0

**Windows 7**
Windows 7 安全更新程序(KB4012212) 下载地址
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212

Windows 7 安全更新程序(KB4012212) 下载（点击图片放大）
Windows 7 x64 （64位）安全更新程序(KB4012212) 下载地址
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212

Windows 7 x64 （64位）安全更新程序(KB4012212) 下载（点击图片放大）

**Windows 10**
Windows 10 安全更新程序(KB4012606) 下载地址
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86\_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu
Windows 10 x64 安全更新程序(KB4012606) 下载地址
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64\_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu
Windows 10 1511 安全更新程序(KB4013198) 下载地址
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013198-x86\_f997cfd9b59310d274329250f14502c3b97329d5.msu
Windows 10 1511 x64 安全更新程序(KB4013198) 下载地址
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013198-x64\_7b16621bdc40cb512b7a3a51dd0d30592ab02f08.msu
Windows 10 1607 安全更新程序(KB4013429) 下载地址
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x86\_8b376e3d0bff862d803404902c4191587afbf065.msu
Windows 10 1607 x64 安全更新程序(KB4013429) 下载地址
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x64\_ddc8596f88577ab739cade1d365956a74598e710.msu

**Windows Server 2008**
Windows Server 2008 安全更新程序 (KB4012598)
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86\_13e9b3d77ba5599764c296075a796c16a85c745c.msu
用于基于 x64 的系统的 Windows Server 2008 安全更新程序 (KB4012598)
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64\_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Windows Server 2008 Itanium 安全更新程序 (KB4012598)
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-ia64\_83a6f5a70588b27623b11c42f1c8124a25d489de.msu

**Windows Server 2008 R2**
基于 x64 的系统的 Windows Server 2008 R2 安全更新程序 (KB4012212)
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64\_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

**其他版本（windows 8.1/windows 2012/windows 2016）安全补丁程序下载地址汇总页**
https://technet.microsoft.com/zh-cn/library/security/MS17-010