关于Absolute公司防盗追踪软件安全风险的提示

一、风险概述

近日，有技术爱好者反映其计算机主板BIOS中预置了一款由Absolute公司开发的防盗追踪软件Computrace，计算机启动后，操作系统即隐蔽安装该软件，经常向境外传输不明数据；该软件可远程获取计算机中用户文件、控制用户系统、监控用户行为，甚至可在未经授权的情况下自动下载安装未知功能的程序，具有很大的安全隐患。

经专家分析发现，Computrace软件预置固化在多款型号计算机BIOS芯片中，软件所使用的网络协议能够提供基础的远程代码执行功能，不需要远程服务器使用任何加密措施或认证，且该远程控制功能随开机启动，常驻于用户电脑，安全风险较大。

二、影响范围

联想、戴尔、苹果、微软、惠普、富士、东芝、松下、三星、华硕、宏基等厂商部分便携式计算机、台式机、工作站。

1. 处置措施

请及时要求有关单位对使用的计算机进行排查，发现预置Absolute公司软件的，请根据业务重要性等妥善处置，方法请参考附件。

附件：

Absolute防盗追踪软件排查与处置方法

一、排查是否

联想品牌计算机请进入BIOS“Security”菜单，查找是否有“Anti-Theft”子项，即如下图所示。



如有“Anti-Theft”子项，进入后可发现Absolute的防盗追踪软件Computrace，即说明存在该软件。



其他品牌请在BIOS菜单中逐一筛查。

二、处置

**方法1：更换主板或升级BIOS**

升级方法请联系计算机生产商咨询。

**方法2：禁止该软件运行**

第一步：打开注册表编辑器，请定位到：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

将右边的 BootExecute 键值（系统默认为autocheck autochk \*）备份后删除掉，阻止该程序自动再启动后续进程。



第二步：在任务管理器中结束相关进程，删除System32目录下的文件rpcnet.exe、rpcnetp.exe、rpcnet.dll、rpcnetp.dll，此时切勿重新启动Windows。

第三步：在System32目录下分别新建以上四个文件，文件内容为空，为每个文件执行如下操作：右键单击，打开属性页，切换到“安全”选项卡，为列出的每个用户或组（包括SYSTEM）设置为拒绝“完全控制”。

**方法3：禁止该软件访问网络**

修改host文件，将相关域名设置为禁止访问：记事本打开C:\Windows\System32\drivers\etc\hosts文件，末行输入以下信息后保存。

127.0.0.1 search.namequery.com

127.0.0.1 search.namequery.com

127.0.0.1 search2.namequery.com

127.0.0.1 search64.namequery.com

127.0.0.1 search.us.namequery.com

127.0.0.1 bh.namequery.com

127.0.0.1 namequery.nettrace.co.za

127.0.0.1 m229.absolute.com

并在防火墙软件中设置将rpcnet.exe、rpcnetp.exe 禁止访问网络。