常见病毒攻击摘要

一、Bluehero挖矿蠕虫变种

该挖矿蠕虫集多种功能为一体，释放后门程序窃取主机信息，释放Mimikatz模块、嗅探模块、“永恒之蓝”攻击模块、LNK漏洞利用模块（CVE-2017-8464）进行传播和反复感染，最终释放挖矿模块进行挖矿。

深信服EDR产品、下一代防火墙及安全感知平台等安全产品均具备病毒检测能力，部署相关产品用户可进行病毒检测。通过深信服提供的免费查杀工具、漏洞补丁及安全云脑，均可有效预防与查杀。

二、虚拟货币挖矿

虚拟货币挖矿是一种复杂的机器运算行为。通常，进行挖矿的矿工需要大规模、高功效的计算设备，进行长时间的运算，从而获取虚拟货币，牟取利益。
早期的比特币等挖矿由于需要大量的密集计算，相比CPU，显卡运算更加快捷和便利，所以一般都有专门搭载高端显卡的设备进行挖矿。然而，近年来兴起的算法CryptoNight是基于AES密集型和很耗内存的算法，这显著降低了GPU对CPU的优势。让CPU挖矿的优势凸显，而以门罗币（XMR）为代表的使用CryptoNight算法的虚拟货币开始流行，黑客看到了其中的商机，投入产出比要比比特币要高的多，所以自2017年以来，黑客通过控制服务器来进行挖矿的行为陡然增多，相关攻击层出不穷。最新发现通过网页进行挖矿。

通常来讲，受害主机存在以下明显的危害：

1、主机长时间执行高性能计算，浪费网络带宽，CPU和内存占用较高，不能及时处理用户的正常请求或任务。
2、增加电力消耗，加快CPU、内存等硬件老化速度。
3、同时挖矿软件已经被植入受害主机，表明主机很可能已被黑客控制，现有的安全防护体系已经部分甚至完全失效，还存在以下潜在风险：
（1）黑客通过挖矿程序窃取机密信息，比如机密文件、关键资产的用户名和密码等，导致企事业单位遭受更进一步的资产损失。
（2）黑客控制主机作为“肉鸡”攻击互联网上的其他单位，违反网络安全法，遭致网信办、网安等监管单位的通报处罚。
（3）黑客利用已经控制的机器，作为继续对内网渗透的跳板，产生更严重的网络安全攻击事件。

主要推荐以下几种方式进行预防与查杀：

1. 深信服EDR分析查杀：<http://edr.sangfor.com.cn/tool/SfabAntiBot.zip>

2、TCPview监控网络，查看谁在与平台标记的矿池服务器进行通信；工具下载链接：<https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview>

3、将定位出的恶意程序，上传到wiki、virustotal等三方机构进行病毒查杀。

三、EnMiner挖矿病毒

EnMiner病毒，是目前遇到的“杀气”最重的挖矿病毒，具有高强度的病毒对抗行为，其病毒机制与常规挖矿相差较大，一旦感染上，清理难度极大，堪称“七反五杀”。能够反沙箱 、反调试、反行为监控、反网络监控、反汇编、反文件分析、反安全分析的同时杀服务、杀计划任务、杀病毒、杀同类似挖矿甚至存在自杀的最大程度反抗分析行为！

主要推荐以下几种方式进行预防与查杀：

1、隔离感染主机：中毒计算机尽快隔离，关闭所有网络连接，禁用网卡。
2、确认感染数量：使用深信服下一代防火墙或者安全感知平台进行全网确认。
3、删除WMI异常启动项：使用Autoruns工具（下载链接为：<https://docs.microsoft.com/zh-cn/sysinternals/downloads/autoruns>），找到异常的WMI启动项，并删除。

4、查杀病毒：推荐使用深信服僵尸网络查杀工具（下载链接为：[http://edr.sangfor.com.cn](http://edr.sangfor.com.cn/)），该工具基于人工智能技术，能够对未知病毒或变种进行有效鉴定，具备检测查杀EnMiner挖矿病毒的能力。

5、修补漏洞：系统若存在漏洞，及时打补丁，避免被病毒利用。
6、修改密码：如果主机账号密码比较弱，重置高强度的密码，避免被爆破利用。