游戏 网络间谍攻击

产品名称	游戏 网络间谍攻击
公司名称	江苏国骏信息科技有限公司
价格	面议
规格参数	
公司地址	徐州市解放南路矿大科技园软件园A座
联系电话	0516-83887908-608

产品详情

江苏国骏--徐州卡巴斯基金牌供应商 资讯：近日，国际知名的信息安全厂商卡巴斯基实验室发表声明，宣布其安全专家团队发现了针对游戏公司的网络间谍攻击，并将关于网络犯罪组织“ winnti ”所发动的一系列持续性网络间谍攻击的详细调查报告公之于众。

根据卡巴斯基实验室报告，winnti组织从2009年开始就对网络游戏行业发动攻击，且目前攻击仍在继续。该组织发动攻击的目的是窃取由合法软件供应商签发的数字证书，此外还会窃取知识产权内容，包括在线游戏项目的源代码。

据了解，发生于2011年秋季的一次安全事件引起了卡巴斯基实验室对winnti组织的恶意行为的注意，当时其在全球大量计算机上检测到一款恶意木马程序。这些受感染计算机之间有一个明显的关联，即这些计算机上都安装了一款流行的网络游戏。之后不久，有细节披露感染这些计算机的恶意程序通过游戏公司的官方服务器进行更新时被感染。受感染用户和该网络游戏社区怀疑是游戏发行公司在消费者计算机上安装了恶意软件，从而监视用户行为。但是，之后的调查显示，这些安装到游戏玩家计算机上的恶意程序是网络罪犯所为，而且他们的攻击目标其实是这家游戏公司。为了解决这一问题，游戏发行公司邀请卡巴斯基实验室对这一恶意程序进行分析。分析表明，该木马是一种针对64位windows环境的dll动态链接库，并且使用了一种合法签名的驱动。该木马是一种功能全面的远程控制工具（rat），能够在计算机用户不知情的情况下，让攻击者完全控制受感染计算机。这次发现意义重大，因为该木马是首个发现的具有合法签名并针对64位windows系统的恶意程序。

卡巴斯基实验室在对winnti组织的恶意行为进行调查时发现网络游戏行业有超过30个公司均遭受到winnti组织的攻击，其中大部分均为东南亚游戏制作公司。除此之外，还有一些位于德国、美国、日本、中国、俄罗斯、巴西、秘鲁和白俄罗斯的在线游戏公司同样成为winnti组织的受害者。除了进行商业间谍行为外，卡巴斯基实验室还发现winnti组织至少可以利用三种手段将窃取到的数据变现，从而生成大量非法利润：

· 操纵和积累游戏内部使用的货币，例如收集游戏玩家的“ 符文“ 或 ”金币“ ，并将积累的虚拟货币转化为真实的钱财；

· 利用从网络游戏服务器窃取到的源代码查找游戏内部漏洞，扩大和加速对游戏货币的控制和积累，并

且不会引起他人察觉；

· 利用从网络游戏服务器窃取到的源代码，搭建自己的私服。

目前，winnti组织的恶意攻击行为仍在继续，卡巴斯基实验室针对其的调查同样正在开展。卡巴斯基实验室的安全专家团队同it安全社区、网络游戏行业和数字证书发放机构正在紧密合作，寻找更多被感染的服务器，同时帮助撤销被盗的数字证书。想要了解卡巴斯基实验室对winnti组织的恶意行为分析的详细报告，包括调查详细技术分析，请访问securelist
http://www.securelist.com/en/analysis/204792287/winnti_more_than_just_a_game

卡巴斯基实验室产品能够完美检测和清除winnti组织使用的恶意程序及其变种，这些恶意程序被命名为as backdoor.win32.winnti、backdoor.win64.winnti、rootkit.win32.winnti和rootkit.win64.winnti。