### **USB HID攻击手段分类及工具**

#### 第一类：微型控制器改编类USB攻击

##### 1、Rubber Ducky

“USB 橡皮鸭”诞生于2010年，是最早的按键注入工具，一直深受黑客、渗透测试人员以及IT专家的欢迎，2010年发布的商业键盘按键注入攻击平台。一旦连接到主机，Rubber Ducky会伪装成电脑病注入预加载的按键序列

最初，橡皮鸭是通过嵌入式开发板实现的，能用简单的脚本语言、强大的硬件进行出色的伪装。

##### **2、PHUKD/URFUKED attack platforms**

PHUKD是「Programmable HID USB Keystroke Dongle」的缩写，它与Rubber Ducky的攻击方式类似，其区别在于这一种, PHUKD式攻击能够让攻击者自由选择注入恶意命令的攻击时间。

##### **3、USBdriveby**

通过模拟USB键盘和鼠标的操作几秒钟内就可以在解锁的OS X主机上安装后门并覆盖原来的DNS设置。

##### **Evilduino**

与PHUKD/URFUKED类似，但使用的是Arduino微控制器而不是Teensy。也是通过模拟键盘、鼠标操作，根据预加载的脚本向主机发送键盘输入或者鼠标移动操作。

##### **Unintended USB通道**

基于Unintended USB通道利用USB硬件木马可以窃取用户数据，比如通过USB扬声器。

##### **TURNIPSCHOOL (COTTONMOUTH-1)**

Cottonmouth-1技术，指的是利用USB嵌入式硬件，让USB插入变成远程窃听或者遥控器的技术。NSA开发的在USB电缆植入的硬件。

##### **RIT attack via USB mass storage（**通过USB大容量存储发起的RIT攻击**）**

这种攻击经常在研究论文中被讨论，当USB大容量存储设备连接到计算机时，通过更改文件内容实施攻击。

##### **Attacks on wireless USB dongles（**对无线USB电子狗的攻击**）**

这个类别的攻击，首先被Samy Kamkar发现，刚好就在他发布KeySweeper那段时间，这是一种能够隐蔽地记录和解密许多Microsoft RF无线键盘击键的工具。

##### **Default Gateway Override（**修改默认网关**）**

使用微控制器欺骗USB以太网适配器以覆盖DHCP设置并劫持本地流量的攻击

#### **第二类：恶意修改USB固件的攻击**

##### **1、**基于智能手机的HID攻击

针对智能手机的HID攻击，首见于论文研究，研究人员自行创建定制的Android小工具驱动程序，然后通过覆盖Android与USB设备交互的方式，让恶意驱动程序与Android USB小工具API交互，从而在连接到手机时，模拟USB键盘和鼠标设备。

##### **2、DNS Override by Modified USB Firmware（**通过修改USB固件的DNS覆写**）**

通过修改USB闪存驱动器的固件，用来模拟USB以太网适配器，然后就能成功劫持本地流量。

##### **3、Keyboard Emulation by Modified USB Firmware（**通过修改USB固件模拟键盘**）**

通过让USB闪存驱动器的固件中毒的方式，然后攻击者就可以模拟键盘，植入命令。

##### **Hidden Partition Patch（**隐藏的分区补丁**）**

将USB闪存驱动器重新编程为正常驱动器，创建无法格式化的隐藏分区，从而实现隐蔽的数据泄露目的。

##### **Password Protection Bypass Patch（**密码保护绕过补丁**）**

对USB闪存驱动器固件的进行一些小改动，攻击者便能绕过有密码保护的USB闪存驱动器，随后可以做其想做的任何事情。

##### **Virtual Machine Break-Out（**虚拟机攻破**）**

使用USB固件来突破虚拟机环境。

##### **Boot Sector Virus（** 引导区病毒**）**

使用USB闪存驱动器，在计算机启动之前进行感染。

##### **iSeeYou**

这也是一种POC程序，对苹果内部iSight网络摄像头固件的重编程，这样攻击者就可以在不触发LED指示器警告的情况下获取视频

#### **第三类：不重编程的USB设备攻击**

##### **1、CVE-2010-2568**

常被Stuxnet和Fanny恶意软件使用的.LNK漏洞，特制的LNK文件可能导致Windows自动执行快捷方式文件所指定的代码。这些代码如果存在于USB驱动中，就会使用资源管理器查看了LNK文件所在位置就足以触发这个漏洞。默认下Windows启动了自动加载和自动播放功能，因此在连接可移动设备(如USB闪存)后Windows会自动打开资源管理器。

##### **2、USB Backdoor into Air-Gapped Hosts**

Fanny恶意软件使用的攻击方式，这种攻击使用USB的秘密存储来存储预置命令，从而能将电脑映射到 air-gapped 网络中，然后该网络上的信息转而又被保存到USB闪存驱动器的隐藏存储中，这种攻击经常会和Fanny恶意软件一同使用。

##### **Data Hiding on USB Mass Storage Devices（**隐藏在USB大存储设备中的数据**）**

隐藏恶意软件或窃取的数据到USB闪存驱动中的技巧和方法，包括把数据存储在正常分区之外、把文件隐藏在不可见的文件夹中。USB闪存驱动器中隐藏恶意软件或被盗数据的大量技巧(例如：将数据存储在正常分区之外，通过将该文件夹的图标隐藏在不可见文件夹中和名称透明等。

##### **AutoRun Exploits（**自动运行利用**）**

根据主机配置的情况，一些计算机会自动执行位于USB设备存储中的预定义的文件，整个恶意软件分类叫做autorun恶意软件。

##### **Cold Boot Attacks（**冷启动攻击**）**

冷启动攻击，又名RAM转储攻击。攻击者可以将存储器转储在USB闪存驱动器中，并通过从USB设备启动来从RAM中提取剩余数据。

##### **Buffer Overflow based Attacks（**缓冲区溢出攻击**）**

当USB设备插入计算机中，许多攻击都是利用OS缓存区溢出。因为USB设备插入设备后，操作系统会枚举设备和函数。

##### **Driver Update（**驱动更新攻击**）**

这种攻击非常复杂，需要获得VeriSign Class 3组织证书并向Microsoft提交驱动程序，从而插入某个SUB设备时，驱动程序会自动发送并安装在用户PC上。这种攻击虽然可行，但在现实世界中很难实现。

##### 设备固件更新Device Firmware Upgrade (DFU)

DFU是USB标准支持的一个合法进程，攻击者可以利用DFU来将本地的合法固件升级为恶意固件。

##### **USB Thief**

是一款基于USB闪存驱动的数据窃取恶意软件

##### **Attacks on Smartphones via the USB Port（**通过USB端口攻击智能手机。**）**

攻击者通过USB电话充电器隐藏和传送恶意软件(恶意)，达到攻击目的。

##### **USBee attack**

使USB连接器的数据总线发出电磁辐射，而这种辐射是用于泄露数据的。

#### **第四类：电子攻击**

##### **1、USB Killer**

通过插入设备，积蓄电容，然后瞬间释放大量电能造成主板烧坏等销毁设备的后果。这种方式不计后果，纯粹以毁坏为目的，性质恶劣，只能从物理层面进行防护。