KCon

返璞归真
重识物理安全与近源渗透

PushEAX

+1 进阶，
护航未来

KCon

+1

CONTENTS

目录

KCon

+1

近源威胁面分析

——虽然只有极少黑客选择在真实世界发起进攻， 但我们面对的威胁远不止与此。

KCon

+1

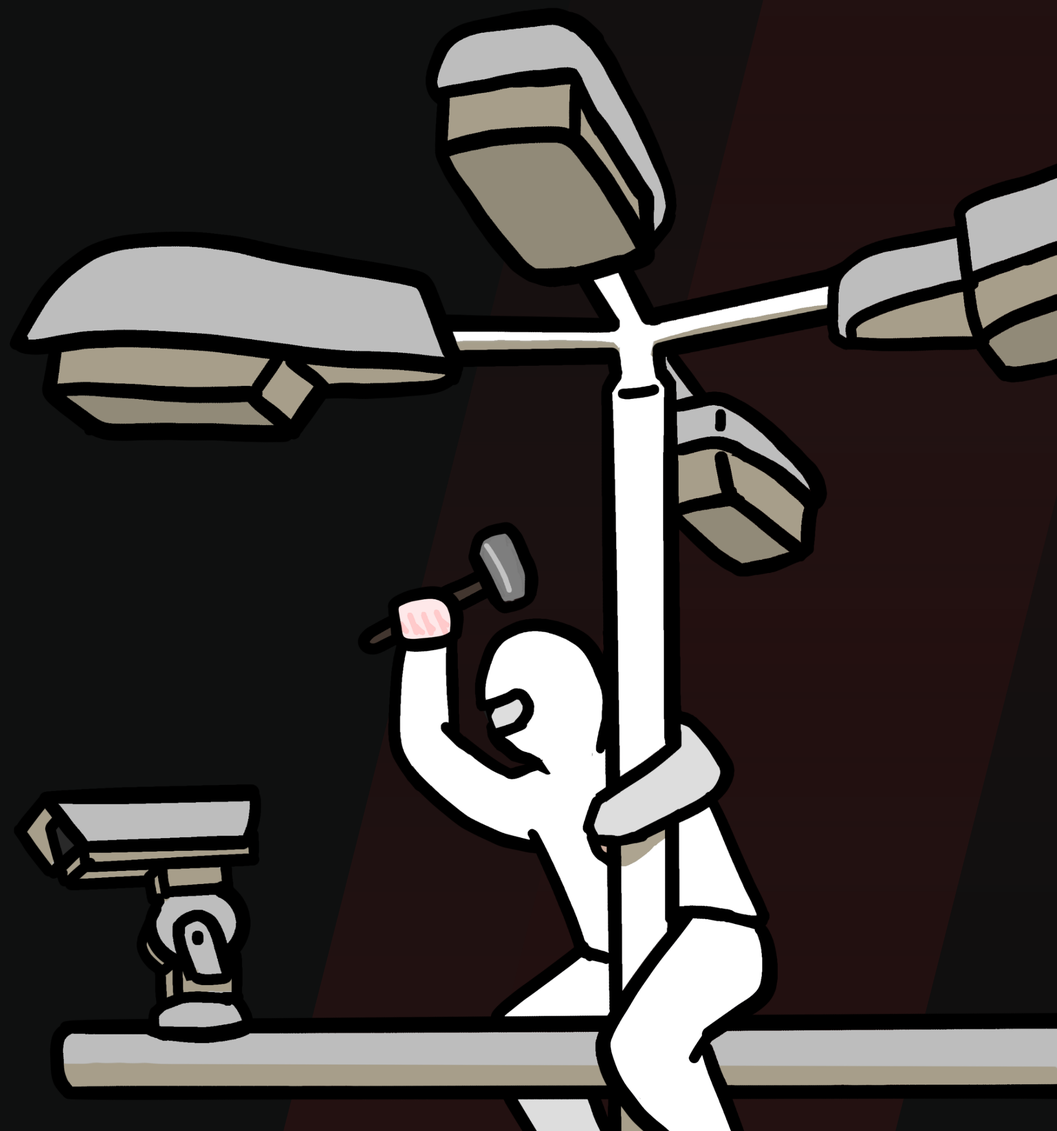
谁会选择在现实世界发起攻击？

黑客攻击(物理)

2007年，网络托管商CI Host的数据中心遭到两名蒙面男子抢劫。劫匪在持枪劫持了一名IT员工后，盗窃了20台服务器。

前员工入侵富士康网络：疯狂洗白iPhone获利300万

攻击者通过贿赂内部员工，在厂区内安装无线路由器。利用无线信号直接连入企业内网，侵入内网中的信息系统。
通过为他人“改机、解锁”手机共9000余部，五个月违法所得300余万元。



KCon

+1

外部威胁

高级黑客 / APT组织 / 间谍

服务提供商 / 硬件供应链

盗窃 / 数据取证

近源威胁

内部威胁

恶意的内部人员

因疏忽或无知造成的威胁

KCon

+1

案例1：五十年前的键盘记录器

1970年代，苏联为窃取机密，在物流阶段截取了美国大使馆的打字机，植入了一个完全由机械结构构造的键盘记录器。

案例2：震网的攻击源自于间谍带入的U盘

荷兰情报机构策反了一名伊朗工程师。将带有病毒的USB闪存驱动器带入了核电站的内部系统。

案例3：淘汰设备泄露数据

2019年，某互联网公司淘汰机房交换机时，未清除设备NVRAM中的配置信息。
泄露了其中的设备登录密码的Hash、内网IP信息、VLAN信息、BGP和OSPF配置等等。

案例4：数据取证技术

案例5：主板内置广告软件

国内外多个笔记本电脑生产厂家，曾被发现在主板的固件程序中内置广告、驱动管理等软件。
即使在更换硬盘并重装系统后，在引导过程中也会被安装特定程序。

KCon

+1

02

近源渗透手段

——近源渗透不止BadUSB

KCon

+1

第一类攻击手段

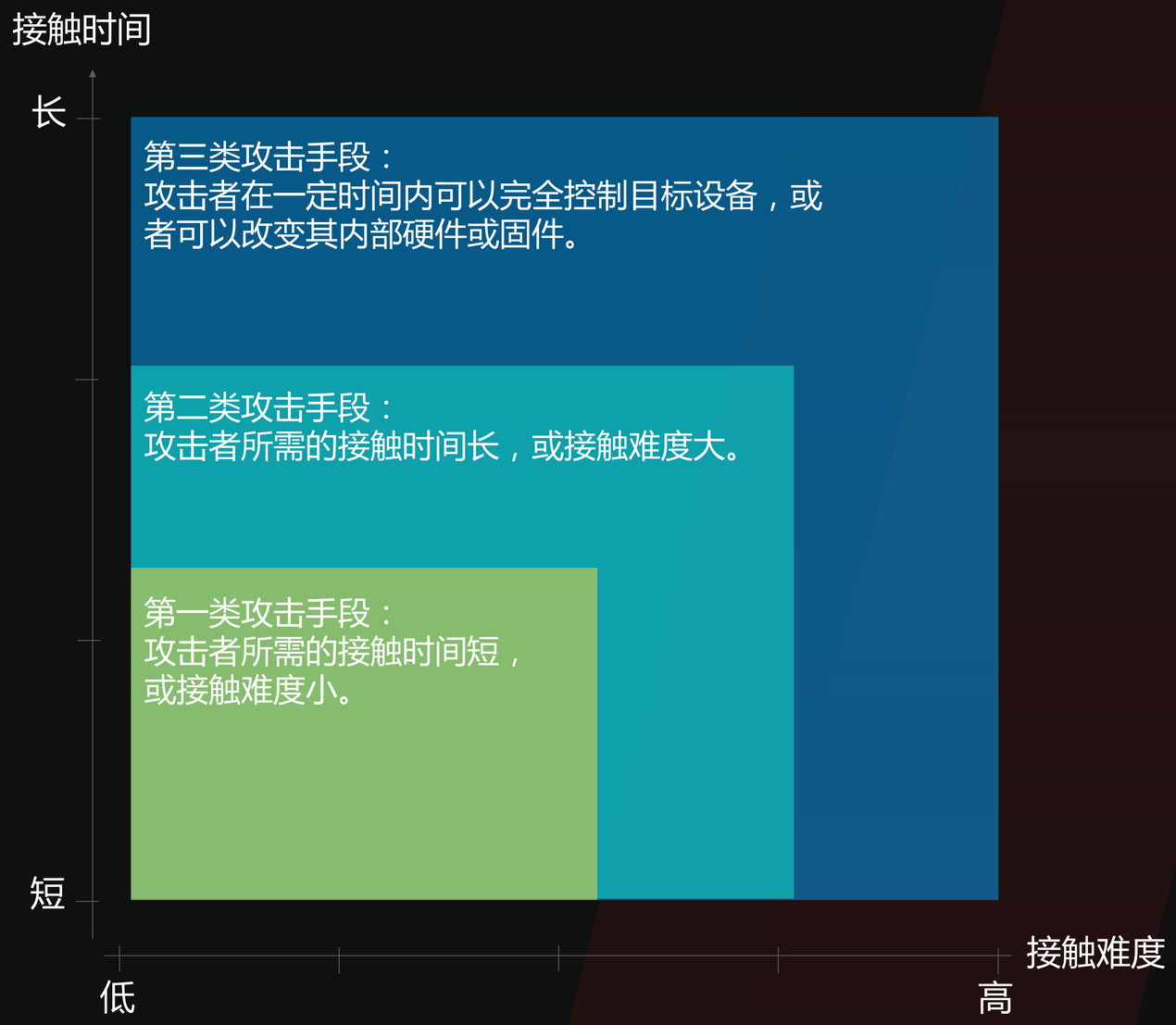
特点：所需的接触时间短，或接触难度小
攻击者：常见为红队成员、外部黑客
目标：钓鱼攻击、无线设备、裸露的接口

第二类攻击手段

特点：所需的接触时间长，或接触难度大
攻击者：带有良好的条件，常见为企业“内鬼”
目标：计算机终端、服务器KVM等

第三类攻击手段

特点：在一定时间内可以完全控制目标设备，或可以改变其内部硬件或固件
攻击者：APT组织、恶意的硬件供应商
目标：硬件设备内部组件、设备固件



KCon

+1

近源渗透手段

KCon

+1

一: 社会工程学攻击

身份伪装

1. 伪装为外卖员、快递员
2. 伪装为面试者、维修工

钓鱼 / 水坑攻击

1. 投递BadUSB及类似设备、植入硬件后门
2. 在公共设备上安装后门

信息收集

1. 盗取访问凭证（工牌图案及UID、文档、公章）
2. 废弃文件、设备的收集

KCon

+1

二: 攻击无线设备

无线网络

1. 跑包握手包 / WPS Pin爆破
2. 钓鱼热点

RFID类设备

1. ID卡的拷贝、爆破
2. IC卡的破解、拷贝

无线电锁具

1. 无线信号的重放攻击

KCon

+1

攻击无线设备——RFID锁具

主要分为ID卡和IC卡

1. ID卡较为古老，但廉价。内部只有一个ID号。
2. IC卡内部有存储器，并且可以加密数据

最广泛使用的是NXP的Mifare系列IC卡

1. 包含1K或4K的存储空间。每张卡有一个UID号
2. 由于存在多个已知漏洞，容易被破解

攻击手段

1. 使用带有NFC功能的手机进行破解
2. 使用PN532进行破解

攻击无线设备——M1卡的破解

结构

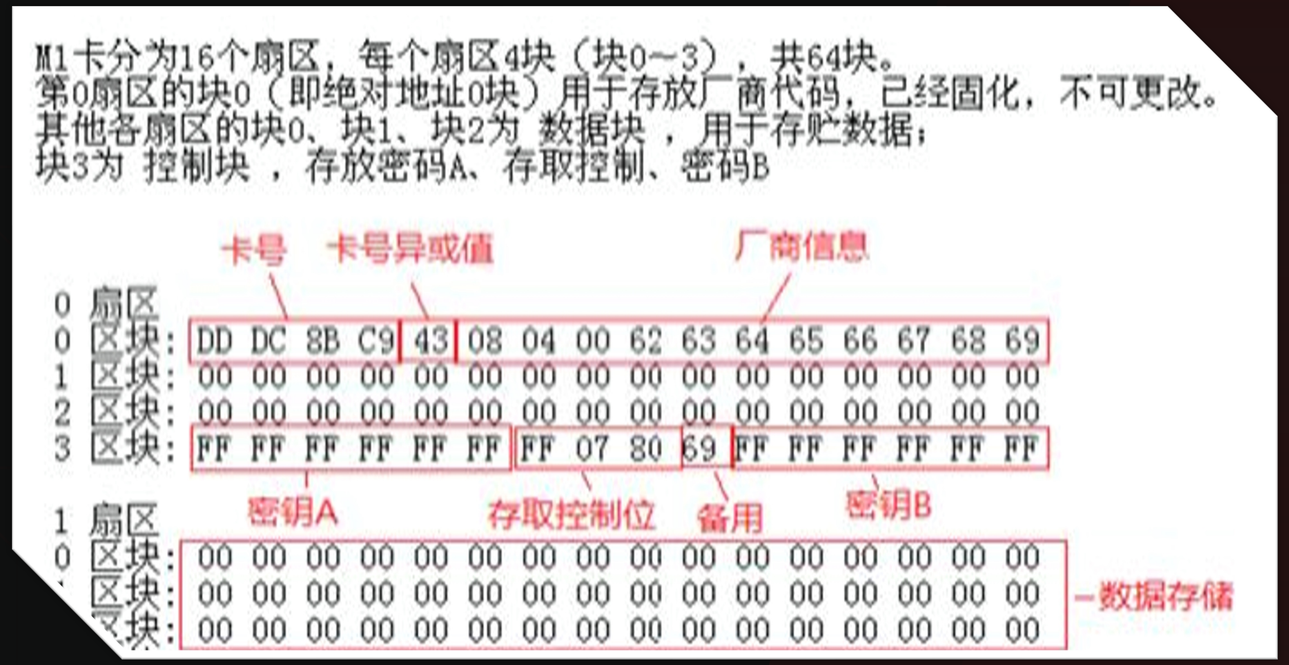
1. 含有1K存储空间
2. 分为16个扇区。每个扇区包含两个访问密钥

UID

1. 扇区0的区块0为厂商信息，原则上只读
2. 扇区0的区块0-3为卡片UID

常见安全问题

1. 门禁只校验UID，造成加密失效
2. 使用默认Key或弱Key



攻击无线设备——无线电锁具

使用无线电遥控的锁具

1. 常见于门禁、车库栏杆
2. 也可用于偷电瓶

通过某个频段的无线电进行通讯

1. 常见为315Mhz、433Mhz
2. 开锁时，遥控器会发送一段“码”

攻击手段

1. 针对固定码，可直接重放攻击
2. 针对滚动码，需要破解出码的生成规律

KCon

+1

攻击无线设备——HACKCUBE

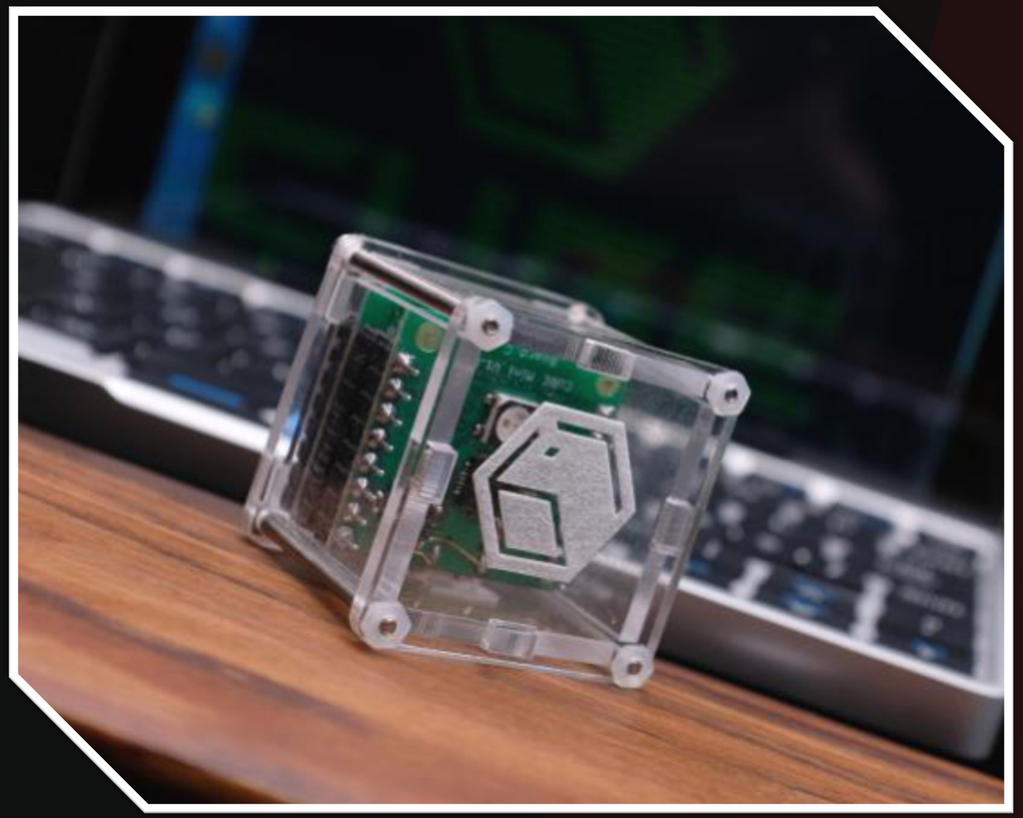
HackCube

开源的无线电审计硬件平台

由360 UnicornTeam开发

功能

1. EM41xx卡的读取和模拟
2. 315、433Mhz无线电信号重放、爆破
3. 通过Wi-fi远程进行HID注入
4. 1Ghz以下频段的干扰



KCon

+1

三: 终端机、裸露接口

终端机的逃逸

1. 双击或长按呼出右键菜单
2. 通过屏幕键盘呼出cmd、Win+D键返回桌面
3. 在网页中存在浏览文件、发送邮件等链接
4. 通过报错，呼出弹窗或使得程序崩溃
5. 可遇不可求的报错或崩溃
6. 直接在设备后面关开关或拔电源线

KCon

+1

三: 终端机、裸露接口

终端机利用

1. 安装木马或开启远程桌面等后门
2. 直接在设备上进行内网渗透
3. 在公用电脑上安装键盘记录器等后门
4. 获取网络配置、应用配置等

终端机、物联网设备、网络设备的裸露接口

1. 通过网口直接进行内网渗透
2. 在网口上安装路由器作为网络后门
3. 通过USB等接口向设备植入木马、盗取数据
4. 通过Console口控制设备
5. 通过UART等接口控制设备

KCon

+1

四: 攻击计算机终端

Kon-Boot（开机密码绕过）

安装在U盘上。
近源渗透时，通过U盘启动计算机，运行Kon-boot。
即可使得Windows密码失效。或安装Shift键后门、添加新账号。

P4wnP1（USB相关攻击）

安装在树莓派上。
多功能的USB攻击工具。
可以模拟为键盘鼠标、网卡、U盘等设备。
可以远程进行HID攻击

WiFiDuck（HID注入或称BadUSB）

硬件设备。
带有Wi-Fi的HID注入设备。
可以通过Wi-Fi操控，执行特定的键盘输入。
用于下载并执行木马、窃取数据等。

PoisonTap（网关劫持）

安装在树莓派上。
插入USB接口后，会伪装成USB网卡，劫持计算机的网关。
可以无视锁屏抓取流量、Cookies，进行缓存投毒。

Windows Lnk代码执行漏洞

安装在U盘上。
当未安装补丁的电脑打开U盘时，即出发任意代码执行。
常用漏洞：
CVE-2020-0729、CVE-2017-8464

Inception / PCILeech（DMA攻击）

安装在带有FireWire接口的计算机上。
近源渗透时，接入目标计算机的FireWire或雷电接口。即可直接读写内存。
可用于植入木马、绕过密码验证等。

KCon

+1

五: 硬件后门

输入/输出设备

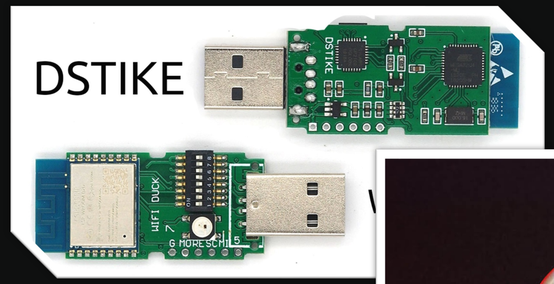
1. 键盘记录器、HID注入设备
2. 屏幕记录器

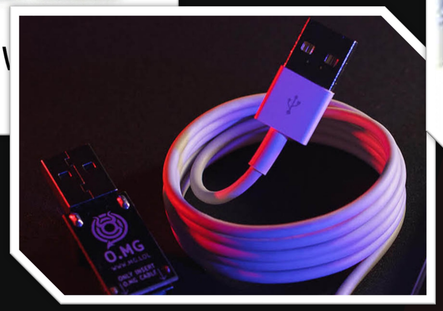
网络相关

1. 内网后门
2. 流量监听

固件篡改

1. 盗取访问凭证（工牌图案及UID、文档、公章）
2. 废弃文件、设备的收集





KCon

+1

ANT Tools工具包介绍

——开源且低成本的近源渗透工具包

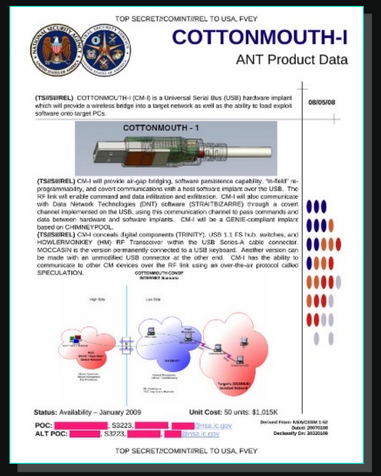
KCon

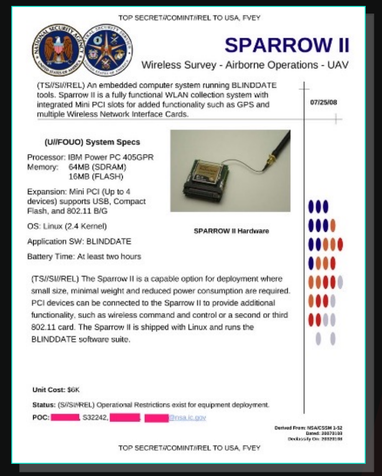
+1

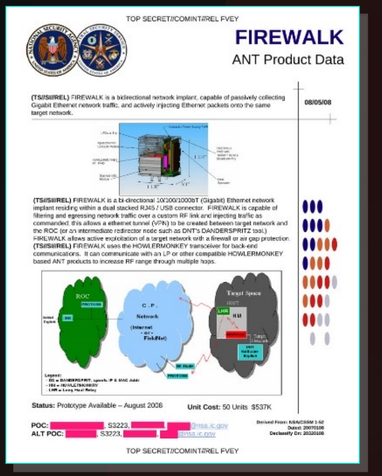
NSA ANT catalog：美国国安局的黑客工具包

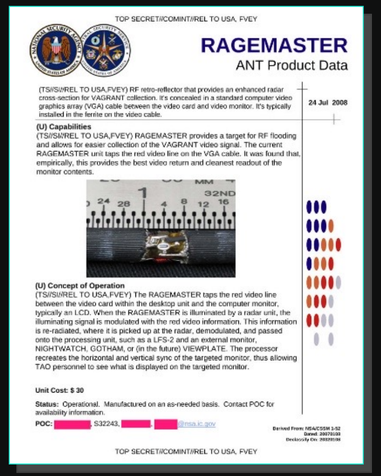
2013年，安全专家Jacob Appelbaum曝光了一份长达50页的NSA机密文档《NSA ANT catalog》，该文档描述了一系列名目繁杂的高端网络黑客攻击技术和项目。

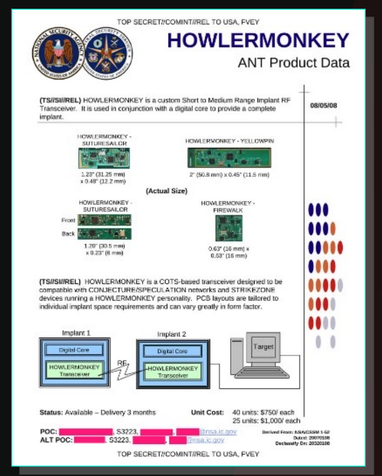
据该文档内容显示，相关的网络黑客攻击技术和项目创建于2008年前后，它们可以认为是为美国国家安全局下属接入技术行动处（TAO）专门定制研发的先进网络攻击武器。

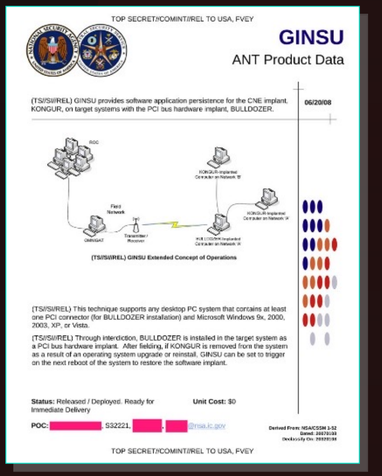












KCon

+1

Hak5: 商业化的硬件渗透测试工具

USB RUBBER DUCKY

A "flash drive" that types keystroke injection payloads into unsuspecting computers at incredible speeds. As seen on Mr. Robot.

by Hak5

Backordered

NEW

BASH BUNNY

A quad-core Linux-box-on-USB-stick mimicking multiple trusted devices to deploy advanced pentest and IT automation payloads.

by Hak5

from $119.99

NEW

SHARK JACK

Jack into a network and instantly run advanced recon, exfiltration, attack and automation payloads.

by Hak5

$69.99

PLUNDER BUG LAN TAP

A pocket-sized Smart LAN Tap with USB-C convenience for passive monitoring or active engagements on wired networks.

by Hak5

Backordered

NEW

KEY CROC

A keylogger armed with pentest tools, remote access and payloads that trigger multi-vector attacks when chosen keywords are typed.

by Hak5

from $109.99

SCREEN CRAB

A stealthy video man-in-the-middle that captures screenshots or videos to disk and streams live to the Internet for remote viewing.

by Hak5

$199.99

KCon

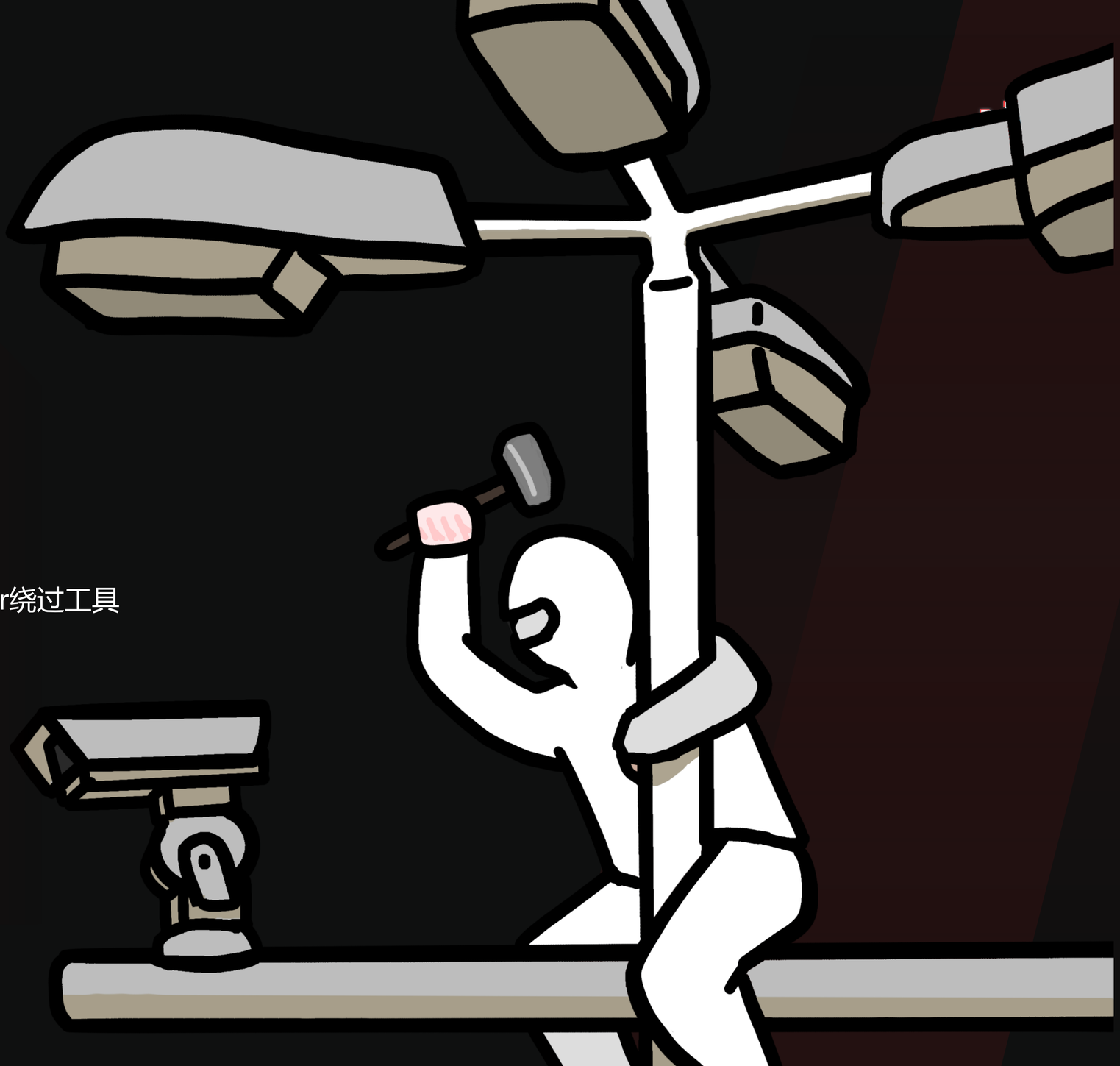
ANT Tools：开源的近源渗透工具包

包含一系列的进攻工具和硬件后门设备

目前计划有：

- USBAirborne： USB钓鱼设备
- GrabAccess： Windows开机密码和Bitlocker绕过工具
- USBKeylogger：硬件键盘记录器

- Telescreen：硬件屏幕记录器
- RadioRaid：无线安全测试平台



KCon

+1

UNCLASSIFIED//SI//REL TO ANT PROJECT

USBAIRBORNE

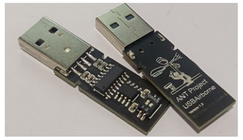
ANT Tool Data

03/13/22

(U//SI//REL) USBAirborne是一个造价极低的近源渗透进攻工具。支持Autorun攻击和BadUSB攻击。

(U) 功能

(U//SI//REL)) USBAirborne是一个近源攻击工具。
USBAirborne可以伪装成U盘，极低的造价使其可以大量投放，用于钓鱼攻击。
在接入受害电脑的USB接口后，可以通过多种方式实现攻击行为。常见的目标有植入木马、执行命令或窃取数据。



(U) 工作原理

(U//SI//REL)
USBAirborne内含一个完整USB Device芯片和一个4MByte Flash。可以模拟为HID设备、USB大容量存储设备。

USBAirborne共有两种攻击方式。
方式一是通过模拟为特殊的DVD-ROM驱动器，绕过Windows Autorun的安全限制，在受害者打开U盘驱动器时，自动执行指定的应用程序。通过模拟为特殊设备，也可以绕过一部分设备禁止使用U盘的安全限制。
方式二是HID注入攻击（又称BadUSB），通过模拟为键盘，执行任意键盘操作，可用于执行任意命令。

USBAirborne也可用作普通存储设备，带有4MB存储空间。

Unit Cost: $2 / each (低于人民币10元/个)

Status: Availability—April 2022

Derived From: ANT Project
Dated: 20220313

UNCLASSIFIED//SI//REL TO ANT PROJECT

UNCLASSIFIED//SI//REL TO ANT PROJECT

GRABACCESS

ANT Tool Data

03/13/22

(U//SI//REL) GrabAccess用于在近源渗透中绕过Windows启动密码和Bitlocker，植入后门或木马程序

(U) 功能

(U//SI//REL)) GrabAccess是一个UEFI恶意程序，安装在U盘上。
在近源渗透中，将带有GrabAccess的U盘插入目标计算机，并从U盘引导，即可运行GrabAccess。
GrabAccess会植入Shift键后门，将Windows粘滞键替换为任务管理器。攻击者在Windows登陆界面即使不登录，也可通过按下五次Shift键呼出任务管理器。用其读写文件、执行任意命令。
GrabAccess也可用于自动安装木马程序，并设置自启动项

(U) 工作原理

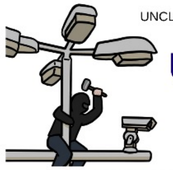
(U//SI//REL) GrabAccess利用了Windows的WPBT（Windows Platform Binary Table）。
WPBT常用于计算机制造商植入驱动软件、防丢软件。类似Bootkit病毒，一旦主板中植入了WPBT条目，无论是重装系统还是更换硬盘，只要使用的是Windows系统，开机后都会被安装指定程序。
WPBT的原始设计是，生产商在主板的UEFI固件中插入一个特定的ACPI条目。Windows引导时，会执行该条目指定的程序。但是，通过劫持UEFI的引导过程，攻击者可以插入WPBT条目，而无需修改主板固件。GrabAccess通过Grab2（Linux的bootloader），实现插入WPBT条目。

Unit Cost: N/A

Status: Availability—April 2022

Derived From: ANT Project
Dated: 20220313

UNCLASSIFIED//SI//REL TO ANT PROJECT



UNCLASSIFIED//SI//REL TO ANTTOOL PROJECT

USBKEYLOGGER-V1

ANT Tool Data

03/13/22

(U//SI//REL) USBKEYLOGGER 是一个硬件后门。安装在USB键盘和计算机之间，记录键盘输入，并提供远程访问功能。

(U) 功能

(U//SI//REL) USBKEYLOGGER 拥有记录键盘输入的能力。并且不需要在目标设备上运行任何程序，只需要接触目标设备一次即可安装。
支持Wi-fi网络功能，可以远程读取记录内容，或自动上传记录内容到指定服务器。目前仅支持USB键盘，未来将提供更微小的可以植入键盘内部或笔记本内部的版本。

(U) 工作原理

(U//SI//REL) USBKEYLOGGER 的一端连接USB键盘，内置的芯片将提供一个USB Host，控制键盘通讯，并将USB-HID协议的按键键入数据转换为UART协议传输给后端的模块。后端的ESP8266模块将会记录键入数据，并提供Wi-fi网络功能。可以通过连接到其开启的热点，读取记录内容。或预先配置其连接到某个热点，并将记录内容上传到预先配置的服务器。最后将由另一个USB芯片提供USB Device，并接入计算机，将获得的数据上传到计算机上。

Unit Cost: $10/each (约合人民币50元/个)

Status: Availability—April 2022

POC: https://www.github.coim/anttool/usbkeyloggerv1

Derived From: Ant Tool Project
Dated: 20220313

UNCLASSIFIED//SI//REL TO ANTTOOL PROJECT

KCon

+1

死去的Autorun突然开始攻击我

Autorun

新设备接入后，自动执行某些操作。

例如插入驱动程序光盘时自动运行安装程序。

现代Windows对Autorun的安全限制

1. 只允许DRIVE_FIXED（固定设备）的CD-ROM驱动器
2. 用Autoplay替代Autorun（受害者必须有交互）

利用方法

1. 伪造一个DRIVE_FIXED的CD-ROM驱动器
2. 在其中放入autorun.inf配置文件

NoDriveTypeAutoRun [edit]

`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

`HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`

Entry name	Data type	Range	Default
`NoDriveTypeAutoRun`	REG_DWORD	0x00 to 0xFF	0x95 or 0x91

KCon

+1

USBAirborne

内置4MB存储空间

通过修改USB DBINQUITY

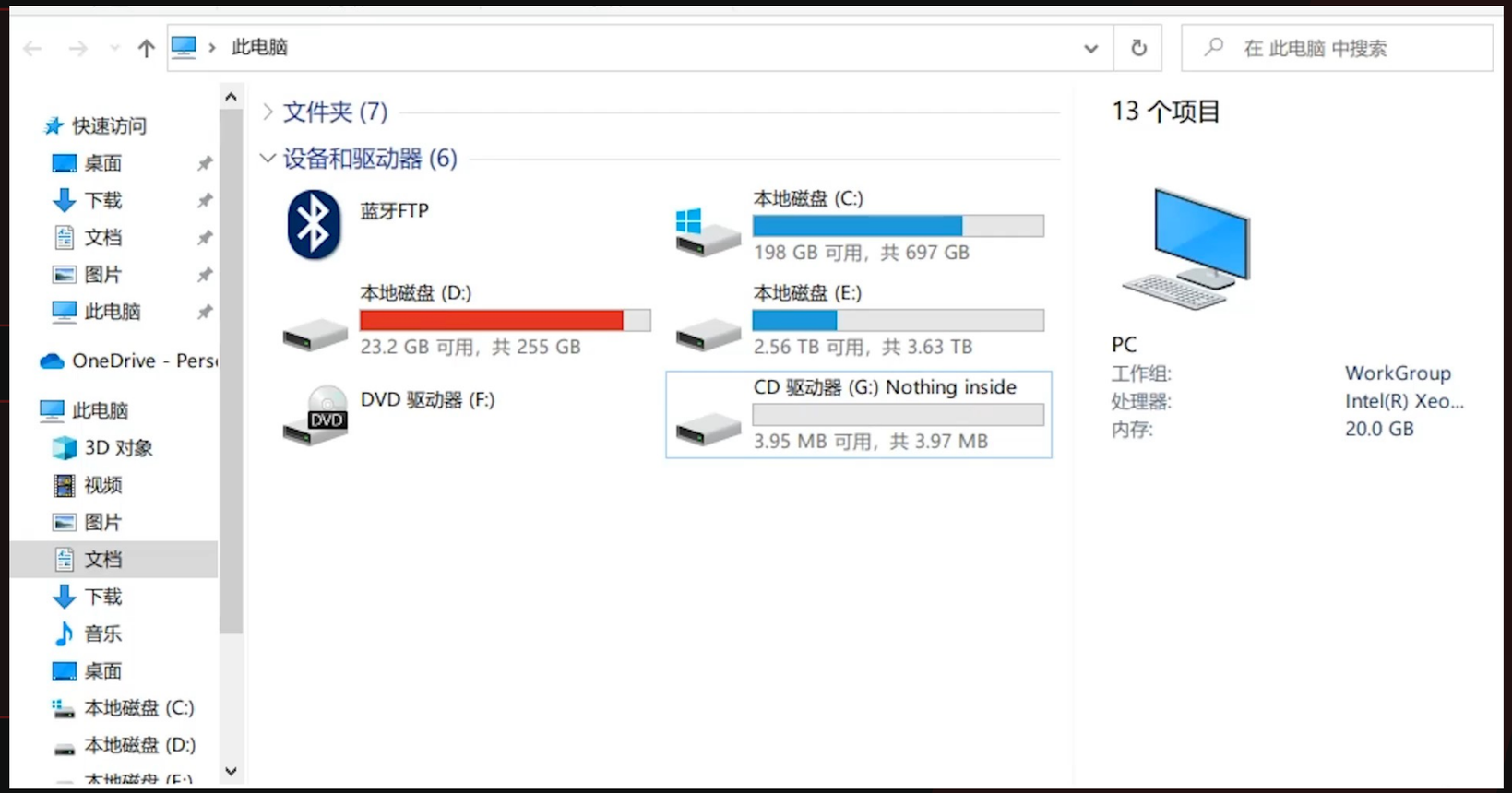
伪装成DRIVE_FIXED的CD-ROM

最终效果

受害者通过任何方

式打开该U盘

即触发Payload



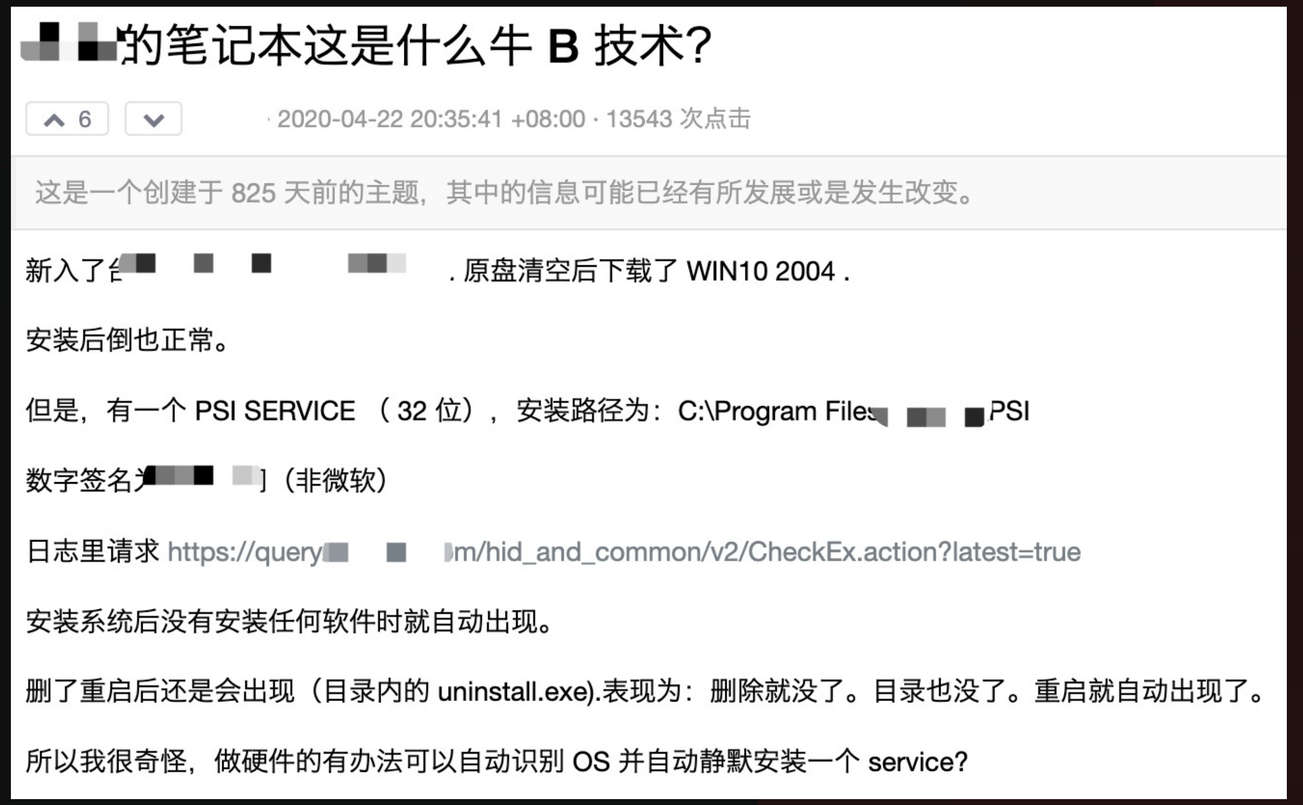
GrabAccess：WPBT的恶意利用

GrabAccess

绕过Widnows登陆密码、Bitlocker植入木马

Windows Platform Binary Table

1. Windows在引导过程中会检查主板的固件。如果存在WPBT条目，则会加载其中的Native Application。
2. 该功能无视Windows登陆密码和Bitlocker。
3. 会对Native App校验签名，但可被绕过。
4. 常用于制造商植入防盗软件、驱动程序。
5. 通过修改UEFI引导过程，可以添加WPBT的ACPI条目。



[redacted]的笔记本这是什么牛 B 技术?

6 · 2020-04-22 20:35:41 +08:00 · 13543 次点击

这是一个创建于 825 天前的主题，其中的信息可能已经有所发展或是发生改变。

新入了台[redacted]. 原盘清空后下载了 WIN10 2004 .

安装后倒也正常。

但是，有一个 PSI SERVICE （32 位），安装路径为：C:\Program Files[redacted]PSI

数字签名为[redacted]（非微软）

日志里请求 https://query[redacted]m/hid_and_common/v2/CheckEx.action?latest=true

安装系统后没有安装任何软件时就自动出现。

删了重启后还是会出现（目录内的 uninstall.exe).表现为：删除就没了。目录也没了。重启就自动出现了。

所以我很奇怪，做硬件的有办法可以自动识别 OS 并自动静默安装一个 service?

KCon

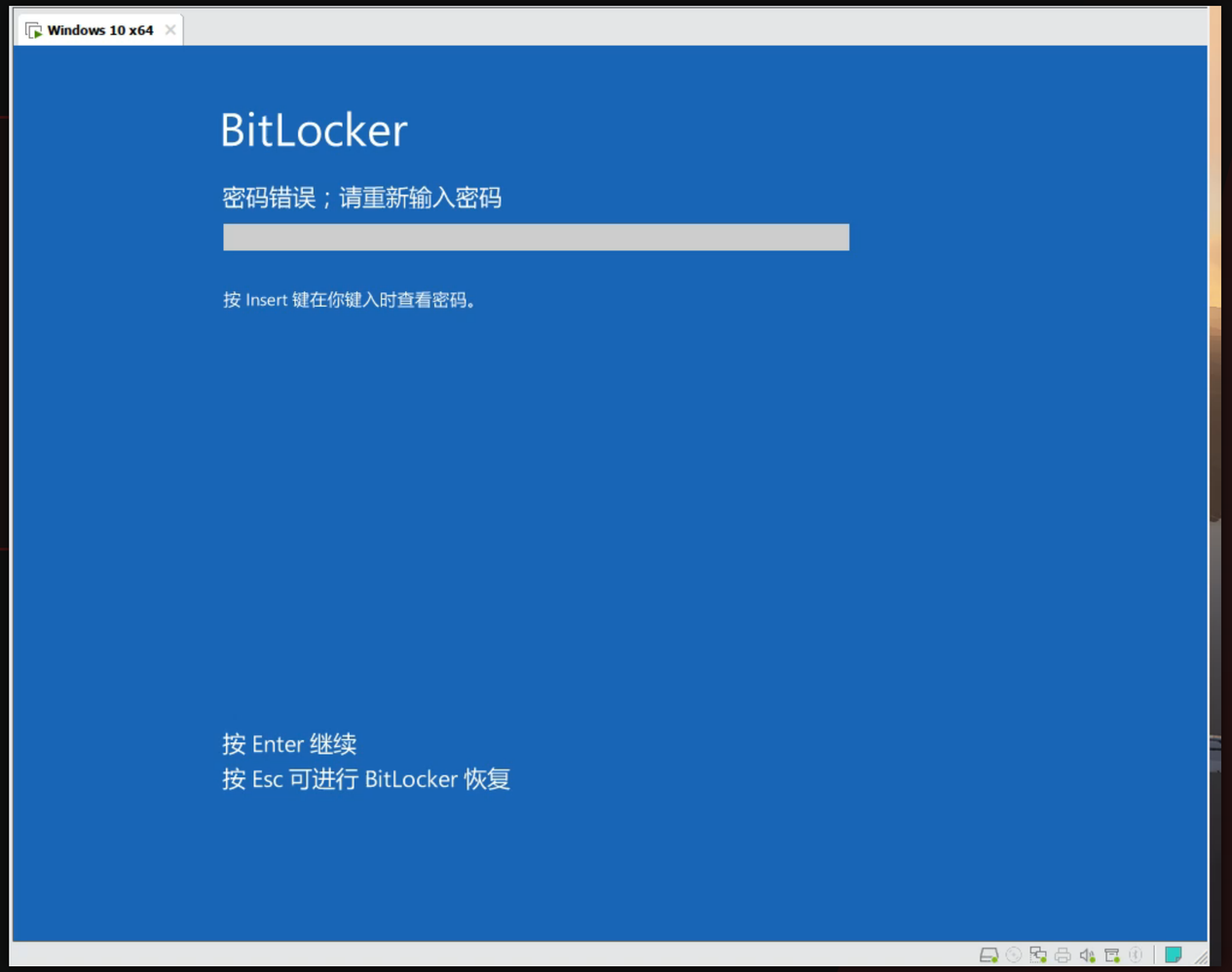
+1

最终效果

将GrabAccess安装在U盘。

近源渗透时将计算机设置为从U盘启动。

正常开机后即会植入木马，或安装Shift键后门



KCon

+1

About Me

杨文韬 @PushEAX

从事信息安全咨询和风险评估工作。

目前致力于近源渗透的理论研究和工具开发。

KCon

+1

感谢您的观看！

THANKYOUFORYOURWANTCHING

KCon 2022 黑客大会