通付盾攻防实验室

网络空间对抗
——基础决定成败

风　宁

kcon2016-西安

网名 ：风宁

80后网络安全爱好者
跨界从散打运动员
转到网络安全从业人员
多年linux 安全、网络apt攻防研究经验

目前在通付盾担任首席安全官及攻防实验室主任

主要负责公司内部网络安全建设、攻防新兴技术研究及产品安全改进！

海湾战争 打印机固件病毒

早在1991年海湾战争中，美军就对伊拉克使用了一些网络战手段。

1990年，美国获悉一个重要情报：
伊拉克将从法国购买一种用于防空系统的新型电脑打印机，准备通过约旦首都安曼偷运回巴格达。
美国间谍买通了安曼机场的守卫人员，运送打印机的飞机一降落到安曼，他就偷偷溜进机舱，
用一套带有计算机病毒的同类芯片换下了电脑打印机中的芯片。伊拉克人毫无察觉，将带有病毒芯片的电脑打印机安装到了防空系统上。
海湾战争爆发后，美国人通过无线网络激活了电脑打印机芯片内的计算机病毒，病毒侵入伊拉克防空系统的电脑网络中，使整个系统陷入瘫痪。

这是世界上首次将计算机病毒用于实战并取得较好效果的战例，从而也使网络空间战初现端倪。
当然，这时的网络战争还不是现代模式的网络攻击，而只是通过病毒进行间接攻击的模式，只能将其看作网络战争的雏形。

KCon West 2016

intel奔腾3序列号后门

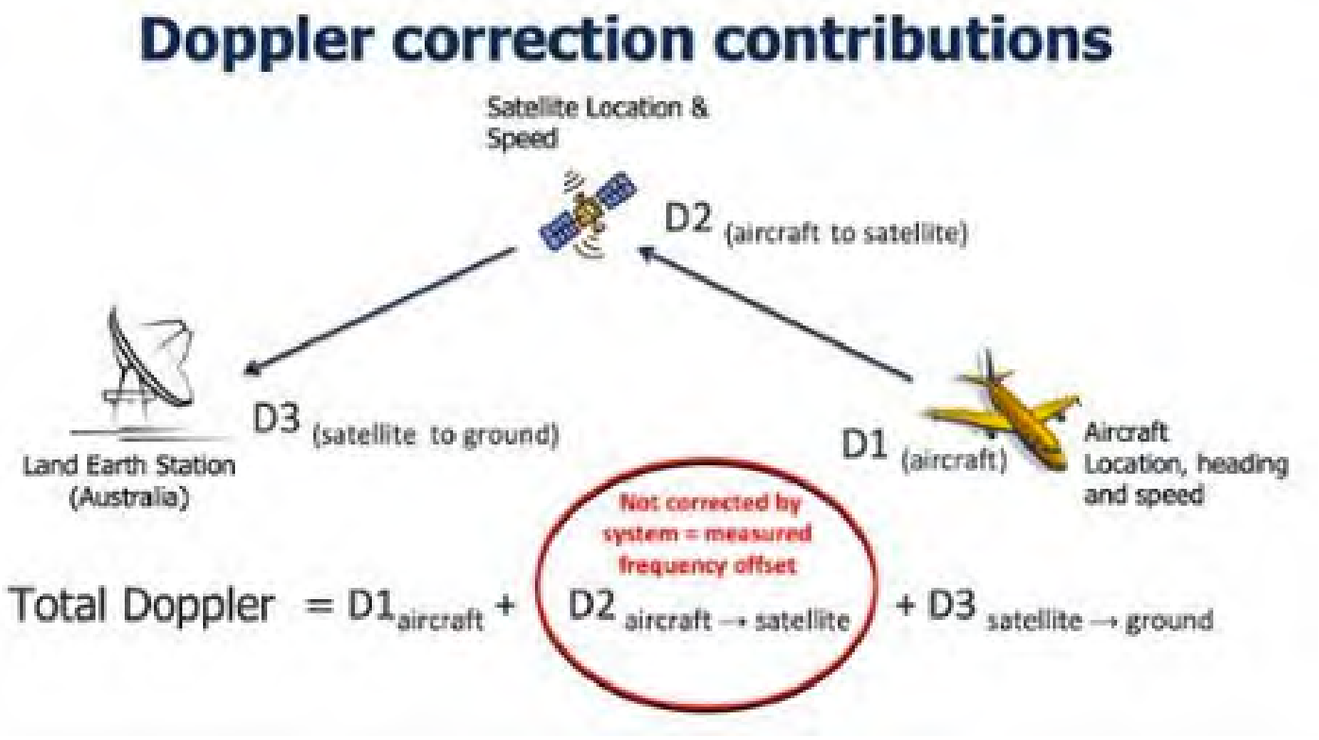
发布者: emma_shao　文档类型: doc

纯文本预览：(跳过预览，直接下载格式良好doc版)

intel 奔腾3 序列号后门
摘自1999 年8 月5 日《电脑日报》)
某一天，忽然有人告诉你，你们单位员工的名字、地址、电话号码出现在某家公
司的数据库里，那家公司还知道你们每天在网上都做了什么事，传送了什么资料
。
如果你安装了奔腾III处理器和Windows98，这种情况就很有可能发生…
微软公司去年推出的操作系统Windows98 和英特尔公司今年2 月推出的微处理
器奔腾III，代表着当今电脑科技发展的最高成就，它们被推崇为最新一代的主流
电脑配置，正在包括中国在内的世界电脑市场上炒得火热。
然而，和以往的每一次技术升级都不同的是，这一次，两家公司在自己的新
产品中不约而同地预留了会泄露用户个人资料的"后门"，奔腾III和Windows98
不仅仅带来了更高的性能和更快的运算速度，更有可能成为埋在用户身边随时会
泄露他们个人资料的"定时炸弹"。

奔III给网上窥视者打开了一扇窗
1 月20 日，英特尔公司宣布为了增强网上电子商务的安全，将在奔腾III处理
器中设置用以识别用户身份的序列码。自那天起，有关序列码的争论一直没有停
息。特别是2 月底奔腾III上市以后，有关奔腾III序列码的争论更加激烈。
英特尔公司增强网上电子商务安全的初衷受到了美国许多民权保护团体的怀
疑，他们认为有了与机器永久相联系的序列码等于是在变相邀请别人窥视自己的
机器，对保障电子交易安全来说没有用处。3 月15 日，美国民主与技术中心(CDT
)向美国联邦贸易委员会(FTC)递交了一份要求禁止奔腾III进入市场的报告，他
们要求FTC 立即采取行动，阻止奔腾III处理器序列码给用户隐私带来的侵害。该组
织要求 FTC 对此展开调查，禁止带有序列码功能的奔腾III处理器进入市场，并禁止
没有关闭序列码功能的奔腾III电脑销售。
反对序列码的人们指出，对序列码的危害绝对不可等闲视之。有了序列码，在网上所做的每一件事都会留下"脚印"。在使用了以奔腾III为中央处理器的电
脑后，员工在互联网络上的一举一动，很可能处在"有心人"的监视之下。"

马航 mf370， 波音 定位事件



Inmarsat（国际海事卫星组织）

6次“握手”

推测出两条可能的最后飞行路线

一条经印度尼西亚至南印度洋

一条自泰国北部至
哈萨克斯坦和土库曼斯坦边境。

打印机固件中存在后门或漏洞

KCon West 2016

PUTTY 汉化版 后门事件

arnetminer.org
B23ACIRDB001.ahe.au.ibm.com
bbs.anbn.cn
bestaor.3322.org
blog.zhengdu.net
bukesiyi.org
capital2.chn.hp.com
cenwor.com
cokebug.gicp.net
co-remote.lboro.ac.uk
dabandeng.com
dev.cpsdna.org
dgcplht.gnway.net
dggclht.gnway.net
dghmlht.gnway.net
dgqslht.gnway.net
dstdb
free.10jsq.com
ftp.yyresolution.com
gdslab01.webex.com
gdsqlht.gnway.net
gzz123.com

neneu.com
new.jk123.com
nextneed.com
nl1.1000usd.info
nyxg.4pu.com
pangpanghu.com
polk.cul.columbia.edu
rcac.xhu.edu.cn
ru1.1000usd.info
ru2.1000usd.info
runcan.gicp.net
rws3220145.us.oracle.com
s1.10jsq.com
s10.10jsq.com
s10.sshwall.com
s11.10jsq.com
s13.10jsq.com
s14.10jsq.com
s7.10jsq.com
s8.10jsq.com
s9.10jsq.com
sangdang.cju.ac.kr

web.sourceforge.net
wohenan.com
www.123flashchat.com
www.33cake.com
www.34358.com
www.36ban.cn
www.csdnstore.com
www.dabandeng.com
www.geilivableit.com
www.goyouqun.com
www.itbl.tk
www.ktvro.net
www.mmxn.com
www.singdiy.com
www.sshcenter.info
www.tangsuanradio.com
www.weibotaobao.com
www.wohenan.com
www.yiki.net
www.zuzhi.com
yiner.biz
youth.ia.ac.cn

PUTTY 汉化版 后门事件

arnetminer.org
B23ACIRDB001.ahe.au.ibm.com
bbs.anbn.cn
bestaor.3322.org
blog.zhengdu.ne
bukesiyi.org
capital2.chn.hp.c
cenwor.com
cokebug.gicp.net
co-remote.lboro
dabandeng.com
dev.cpsdna.org
dgcplht.gnway.n
dggclht.gnway.n
dghmlht.gnway.
dgqslht.gnway.n
dstdb
free.10jsq.com
ftp.yyresolution.
gdslab01.webex.
gdsqlht.gnway.net
gzz123.com

neneu.com
new.jk123.com
nextneed.com
nl1.1000usd.info

web.sourceforge.net
wohenan.com
www.123flashchat.com
www.33cake.com

中文版putty后门事件分析

2012-02-01 17:45:24 9904 次阅读 21 次推荐 稿源: 0 条评论

感谢lszm的投递

近几日，中文版putty等SSH远程管理工具被曝出存在后门，该后门会自动 窃取管理员所输入的SSH用户名与口令，并将其发送至指定服务器上。知道创宇安全研究小组在第一时间获取该消息后，对此次事件进行了跟踪和分析。根据分 析，此次事件涉及到来自putty.org.cn、putty.ws、winscp.cc和sshsecure.com站点的中文版putty、 WinSCP、SSHSecure和psftp等软件，而这些软件的英文版本不受影响。

1．时间线

1月25日：新浪微博有网友发布消息称putty和winscp中装有后门程序，但该条微博并未提及后门程序的类型及其技术细节，而且消息也未被过多的人所重视，目前无法确定该条微博是否与此次事件有关联:

s8.10jsq.com
s9.10jsq.com
sangdang.cju.ac.kr

yiner.biz
youth.ia.ac.cn

国内外“黑客”工具系列

Gh0st控制端远程堆溢出

wireshark 堆溢出

Poison Ivy 远程溢出

中国菜刀-工具后门

Acunetix WVS 远程执行

Necat

Nmap

HFS 远程溢出

mIRC 远程溢出

BackTrack 5

安全防护软件

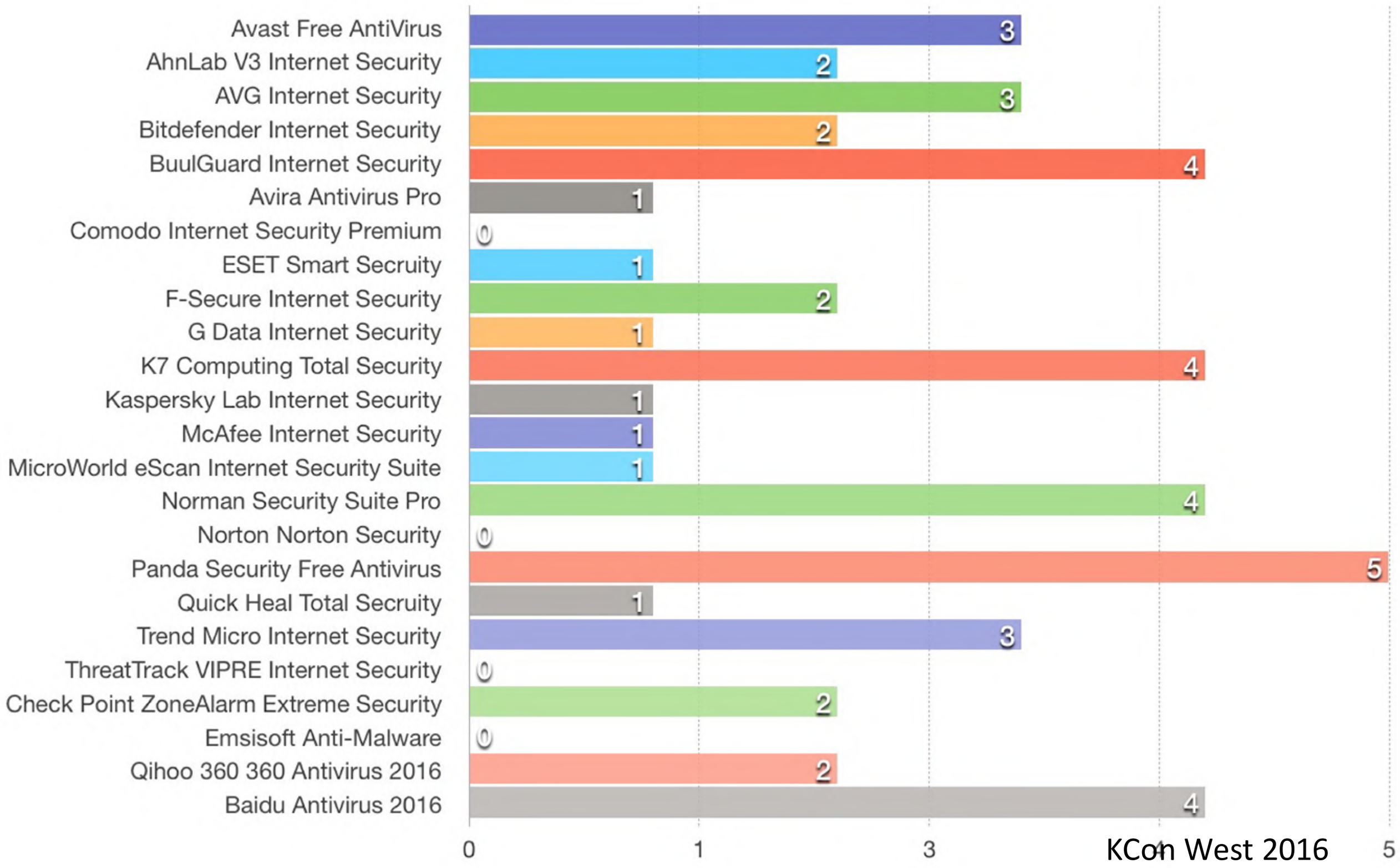
openssl 心脏滴血

FortiGate OS(飞塔系统) 4.0-5.0.7 SSH 后门

全球各大杀软应用漏洞

KCon West 2016

安全防护软件



KCon West 2016

BGP—网络空间的核武攻击

2010年4月10日星期六

中国ISP又一次劫持了互联网 zz

过去两周内的第二次，从中国传播出去的错误网络信息让 整个互联网出现混乱。

本周四早晨，一家叫IDC China Telecommunication的小型ISP的错误路由数据，经过中国电信的二次传播，扩散到了整个互联网，波及到了 AT&T、Level3、Deutsche Telekom、Qwest Communications和Telefonica等多个国家的大型ISP。事故始于美国东部时间上午10点，持续了大约20分钟。在此过程中，有32,000到37,000个网络接收到了错误的数据，包括8,000个美国网络，超过8,500个中国网络，1,100个澳大利亚网络，230个法国网络。

细节：
IDC China Telecommunication为32,000到37,000个网络传送了错误的路由信息，将他们指向了自身而不是正确的地址。

These networks included about 8,000 U.S. networks including those operated by Dell, CNN, Starbucks and Apple. More than 8,500 Chinese networks,1,100 in Australia and 230 owned by France Telecom were also affected.

While the incident appears to have been an accident, it underscores the weakness of the Border Gateway Protocol (BGP), a critical, but obscure, protocol used to bind the Internet together.
（中文译文：当这一事件演变成一场事故，又暴露出BGP协议的缺陷，就是这个关键但是又模糊的协议将Internet捆绑在一起）

BGP data is used by routers to tell them how to route traffic over the Internet. Typically smaller service providers "announce" BGP routes for the networks they control, and that information is ultimately centralized and then shared between larger providers. That's where the problems started on Thursday. For some reason, IDC China Telecommunication announced routes for tens of thousands of networks -- about 10 percent of the Internet. Typically this small ISP announces about 30 routes.
（中文：路由器通过BGP数据来控制如何在Internet上转发流量。一般是小的运营商为它控制的网络来声明路由信息，这些信息被集中，然后在大的运营商之间共享。IDC China Telecommunication为数万个网络来声明路由，大概占到Internet的10%。）

BGP—网络空间的核武攻击

46.166.163.175

2010年4月10日星期六

中国ISP又一次劫持了互联网

过去两周内的第二次，从中国传播出去的错误网络信息让整个互联网出现混乱。

本周四早晨，一家叫IDC China Telecommunication的小型ISP的错误路由数据，经过中国电信的二次传播，扩散到
Telef
32,0
大利亚

细节：Hacking Team雇员之间的电子邮件通信显示，该公司曾在2013年通过伪造BGP路由广播劫持了一个IP段。
IDC
是正

Thes
Starb
Franc

While
Gate
（中
Inter

Hacking Team通过虚假BGP路由广播劫持IP段

WinterIsComing (31822)发表于 2015年07月13日 16时21分 星期一

来自应该多嵌入几个指令控制服务器地址才对部门

Hacking Team向执法机构和情报机构出售远程控制工具，它的一个客户是监视有组织犯罪和恐怖主义的意大利国家军事警察的特别行动组，特别行动组利用钓鱼邮件等手段让远程控制工具感染目标的计算机，远程控制工具通过指令控制服务器记录按键和通信，上传收集的数据，收集目标的各种信息。2013年8月特别行动组失去了对指令控制服务器（IP地址46.166.163.175）的访问，原因是在一系列宕机事件后主机托管商Santrex（自治编号AS57668）的IPv4前缀46.166.163.0/24永久性无法访问（Santrex在当年10月破产）。为了恢复对服务器的访问，特别行动组寻求Hacking Team的帮助。Hacking Team与意大利网络运营商Aruba S.p.A（AS31034 ）合作，通过BGP路由广播向对等网络宣布它拥有46.166.163.0/24地址段，在对等网络接受之后，46.166.163.175地址再次可以访问。Aruba是在8月16日劫持该地址段，8月22日撤回了路由广播，显然特别行动组已成功修改了远程控制工具的配置，使其可以连上其它IP地址。这是已知的第一起ISP欺骗性的宣布拥有另一家供应商IP地址的案例。

BGP data is used by routers to tell them how to route traffic over the Internet. Typically smaller service providers "announce" BGP routes for the networks they control, and that information is ultimately centralized and then shared between larger providers. That's where the problems started on Thursday. For some reason, IDC China Telecommunication announced routes for tens of thousands of networks -- about 10 percent of the Internet. Typically this small ISP announces about 30 routes.

（中文：路由器通过BGP数据来控制如何在Internet上转发流量。一般是小的运营商为它控制的网络来声明路由信息，这些信息被集中，然后在大的运营商之间共享。IDC China Telecommunication为数万个网络来声明路由，大概占到Internet的10%。）

传说中的3389远程溢出？

MS15-085中的漏洞涉及所有支持版本的Windows中的Mount Manager，如果攻击者插入恶意USB设备到目标系统，然后写入恶意二进制到磁盘并执行，这可能允许特权提升。

对于这个漏洞的严重程度，专家们存在争议，微软将该漏洞标记为“重要”，这通常意味着该漏洞比“严重”漏洞更难以被利用。但该漏洞已经被公开利用，这让一些专家认为这是本月安全公告中的重要漏洞。但Young表示，该漏洞没有看起来那么容易被利用。

“我的第一反应是，这可能是另一个pwn漏洞，例如针对伊朗核计划的Stuxnet攻击中使用的LNK漏洞利用。然而，在仔细分析后，我发现这完全不是一回事，”Young称，“这很容易被本地攻击者用来执行DLL或二进制劫持攻击，以在系统允许下执行代码，但这似乎不会为系统提供攻击向量来在插入USB时自动感染系统。此外，似乎攻击者不能利用该漏洞来获得锁定系统的权限，因为没有自动代码执行。”

Young还指出，虽然MS15-082涉及远程桌面协议中的漏洞—这可能允许远程代码执行，但微软将该公告评为“重要”而不是“严重”，这里有一定的原因。

“对于MS15-082中的漏洞，如果攻击者已经有一定程度的访问权来将DLL文件加载到受害者当前工作目录然后加载.RDP文件，那么攻击者可能实现‘远程’代码执行，”Young表示，“虽然这可能应用于实际攻击，但这需要与用户一定水平的交互来成功执行攻击。”

传说中的3389远程溢出？

哥今天让传说重现^__^

約 33,400 項搜尋結果 (0.54 秒)

VDI序曲十四使用RemoteFX 安装和配置USB 重定向- ZJUNSEN的微软 ...
rdsrv.blog.51cto.com/2996778/563271 ▾ 轉為繁體網頁
2011年5月10日 - RemoteFX重定向USB功能介绍：用户应该能够使用任何工作中的设备。 ... 计算机配置\策略\管理模板\Windows 组件\远程桌面服务\远程桌面连接 ...

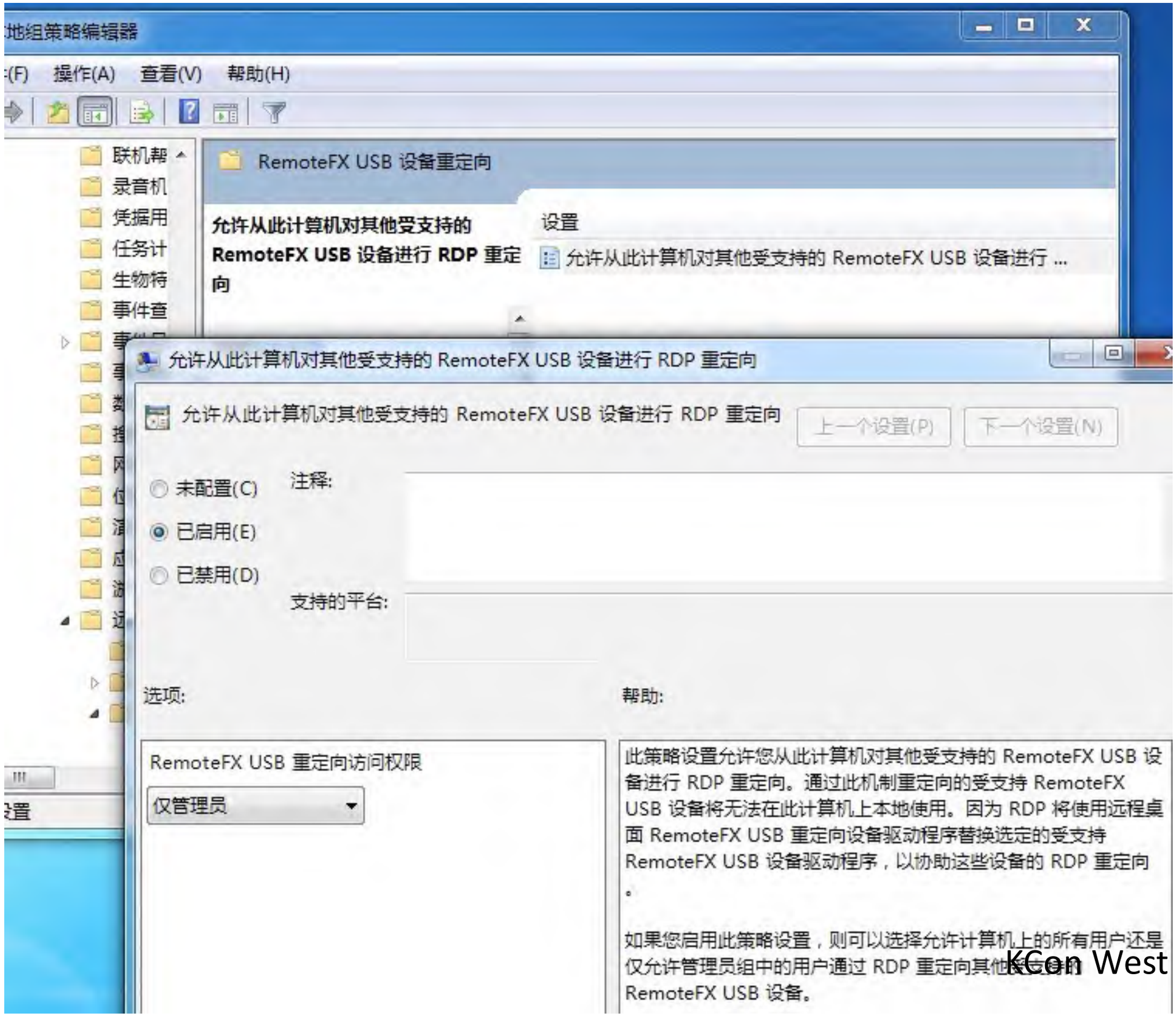
Microsoft RemoteFX - TechNet
https://technet.microsoft.com/zh-cn/library/ff817578(v=ws.10).aspx ▾ 轉為繁體網頁
有关RemoteFX USB 重定向的详细信息，请参阅 使用RemoteFX 的逐步式指南配置USB 设备重定向 rdp-tcp？LinkId = 192431） Windows Server 2008 R2 技术库上 ...

VDI序曲十四使用RemoteFX 安装和配置USB 重定向_百度文库
wenku.baidu.com/view/3a1a4c7faf1ffc4ffe47ac32.html?re=view - 轉為繁體網頁
2013年6月14日 - VDI序曲十四使用RemoteFX 安装和配置USB 重定向_计算机软件及 ... 管理模板\Windows 组件\远程桌面服务\远程桌面连接客户端\RemoteFX USB ...

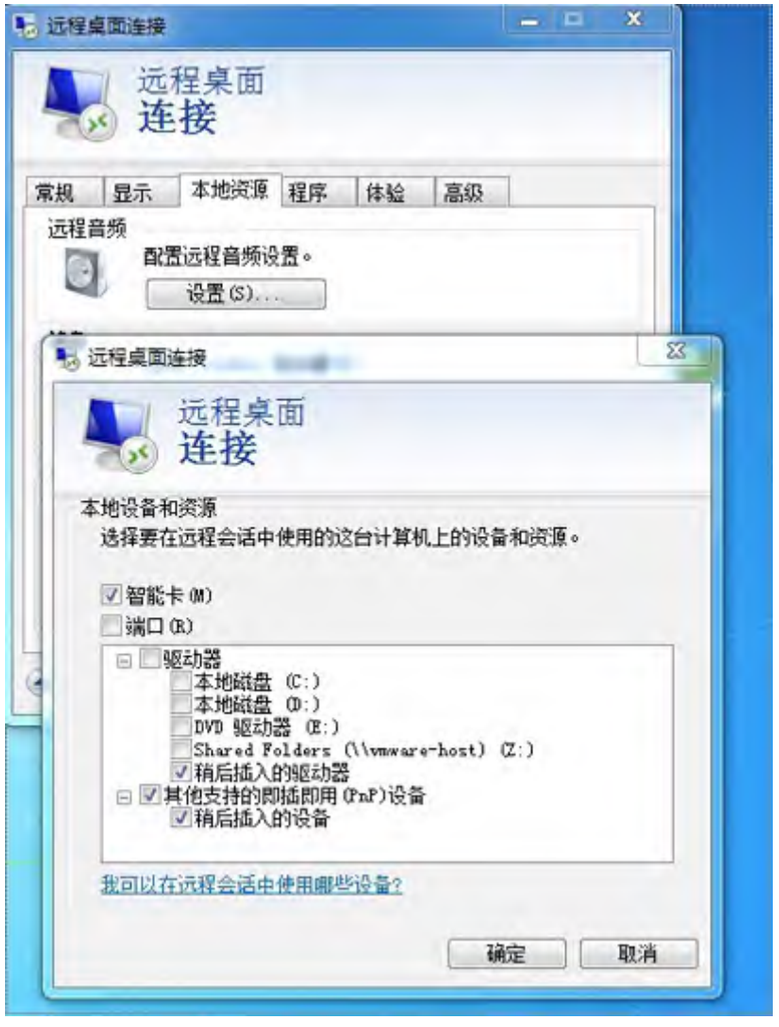
RemoteFX USB的无法重定向本地USB设备-CSDN论坛-CSDN.NET ...
bbs.csdn.net › CSDN论坛 › Windows专区 › 网络管理与配置 ▾ 轉為繁體網頁
2013年3月23日 - 计算机配置 \ 管理模板 \windows 组件 \ 远程桌面服务 \ 远程桌面连接 ... 启用【允许来自此计算机的设备的其他受支持的 RemoteFX USB RDP 重 ...

KCon West 2016

传说中的3389远程溢出？



传说中的3389远程溢出？



^

KCon West 2016

APT攻防领域，需要持续跟踪研究
8月KCon北京见！

KCon West 2016