Windows密碼抓取工具

手機黑客 昨天

> **文章作者：Luckysec**
> **原文鏈接：**
> **http://luckyzmj.cn/posts/9686fbeb.html**

前言

本篇介紹幾款優秀的Windows上的密碼抓取工具，每個工具都有自己的特點非常實用，歡迎補充。

0x01 模仿

> 個人點評：這款工具非常強大，公認的Windows密碼神器。

1. 簡介

Mimikat是一個法國人寫的輕量級調試器。Mimikat可以從內存中提取純文本密碼，hash，PIN碼和kerberos票證。mimikatz還可以執行哈希傳遞，票證傳遞或構建Golden票證
項目地址：https://github.com/gentilkiwi/mimikatz/

2. 使用
cmd運行命令如下：

```
mimikatz.exe # cmd命令执行启动程序
privilege::debug # 提升权限
sekurlsa::logonpasswords # 抓取密码
```

> Mimikatz 功能非常強大，這裡只簡單介紹了常用的抓取密碼命令。

0x02 BrowserGhost

> 個人點評：這款工具的亮點就是可以不用輸入windows系統密碼，直接提取谷歌瀏覽器中存儲的密碼。

1. 簡介

這是一個抓取瀏覽器密碼的工具，後續會添加更多功能，已經完成的功能如下：

實現system抓機器上其他用戶的瀏覽器密碼(方便橫向移動時快速憑據採集)

用.net2 實現可兼容大部分windows，並去掉依賴(不需要System.Data.SQLite.dll這些累贅)

可以解密chrome全版本密碼(chrome80版本後加密方式變了)

Chrome已經可以獲取login data、cookie、history、book了

IE 支持獲取書籤、密碼、history了(.net2提取密碼太複雜了代碼參考至https://github.com/djhohnstein/SharpWeb/raw/master/Edge/SharpEdge.cs)

項目地址：https://github.com/QAX-A-Team/BrowserGhost

2. 使用

cmd運行如下命令：

```
BrowserGhost.exe
```

0x03 SharpDecryptPwd

> 個人點評：這款工具的亮點是可以提取一些windows上常用的第三方程序進行解析提取存儲的密碼。

1. 簡介

對密碼已保存在Windwos 系統上的部分程序進行解析,包括：

Navicat,TeamViewer,FileZilla,WinSCP,Xmangager系列產品（Xshell,Xftp)。

項目地址：
https://github.com/uknowsec/SharpDecryptPwd

2. 使用

cmd運行如下命令：

```
SharpDecryptPwd.exe
SharpDecryptPwd.exe -TeamViewer
SharpDecryptPwd.exe -NavicatCrypto
SharpDecryptPwd.exe -FileZilla
SharpDecryptPwd.exe -Xmangager -p D:\xshell\Xshell\Sessions

# Cobalt Strike
execute-assembly /path/to/SharpDecryptPwd.exe
```

0x04 拉扎涅

> 個人點評：這款工具可以一鍵抓取本地計算機上的所有明文密碼，可獲取的軟件密碼種類非常多，支持Windows、Linux、Mac。

1. 簡介

LaZagne是用於開源應用程序獲取大量的密碼存儲在本地計算機上。每個軟件使用不同的技術（純文本，API，自定義算法，數據庫等）存儲其密碼。開發該工具的目的是為最常用的軟件找到這些密碼。該項目已作為開發後模塊添加到pupy中。Python代碼將在內存中解釋而無需接觸磁盤，並且可以在Windows和Linux主機上運行。

項目地址：
https://github.com/AlessandroZ/LaZagne

2. 使用

安裝依賴庫

```
pip3 install -r requirements.txt
```

一鍵獲取所有支持的類型密碼

```
python3 lazagne.py all
```

支持的類型密碼如下：

類型	視窗	Linux	蘋果電腦
瀏覽器	7Star,Amigo,BlackHawk,Brave,Centbrowser,Chedot,Chrome Canary,Chromium,Coccoc,Comodo Dragon,Comodo IceDragon,Cyberfox,Elements Browser,Epic Privacy Browser,Firefox,Google Chrome,Icecat,K-Meleon,Kometa,Opera,Orbitum ,人造衛星,TorchUran,Vivaldi	勇敢、鉻、異議瀏覽器、谷歌瀏覽器、IceCat、火狐、Opera、SlimJet、Vivaldi、WaterFox	鉻、火狐
貓	Pidgin，Psi，Skype	皮金，Psi	
數據庫	DBVisualizer、Postgresql、Robomongo、Squirrel、SQLdevelopper	DBVisualizer、Squirrel、SQLdevelopper	
遊戲	GalconFusion、Kalypsomedia、RogueTale、Turba		
走	適用於 Windows 的 Git		
郵件	展望，雷鳥	爪甲、雷鳥	
馬文	阿帕奇		
從內存中轉儲	Keepass,Mimikatz 方法	系統密碼	
多媒體	眼控		
PHP	作曲家		
SVN	烏龜		

類型	視窗	Linux	蘋果電腦
系統管理員	Apache Directory Studio、CoreFTP、CyberDuck、FileZilla、FileZilla Server、FTPNavigator、OpenSSH、OpenVPN、KeePass 配置文件（KeePass1、KeePass2）、PuttyCM、RDPManager、VNC、WinSCP、		
適用於 Linux 的 Windows 子系統	Apache Directory Studio,AWS,Docker,Environnement variable,FileZilla,gFTP,History files,Shares,SSH private keys,KeePass Configuration Files (KeePassX, KeePass 2),Grub		
無線上網	無線網絡	網絡管理員，WPA 請求方	
內部機制密碼存儲	Autologon,MSCache,Credential Files,Credman,DPAPI Hash,Hashdump (LM/NT),LSA secret,Vault Files	GNOME 鑰匙圈、Kwallet、Hashdump	鑰匙串，Hashdump

侵權請私聊公眾號刪文