PASSWORD SECRETS OF POPULAR WINDOWS APPLICATIONS

F4RY4R_RED & X3N0N

UNKNOWN SECURITY DIGITAL TEAM

www. hackfans.org

بسمه تعالی

اسرار رمز عبور در نرم افزار معروف ویندوز

مقدمه

در دنیای اینترنت محور امروز، همه ما با استفاده از یک یا چند برنامه کاربردی از مرورگرها، سرویس های ایمیل و بسیاری از این برنامه ها به ذخیره اطلاعات حساس خود مانند نام کاربری، رمز عبور در محلهای خاصی با استفاده از روش های اختصاصی می پردازیم ، با گمان اینکه با این کار از ورود به حسابهای کاربری خودمان جلوگیری می کنیم.

با این حال آنچه مهم است که بدانیم ، این اطلاعات محرمانه در صورتی که در دست کسی دیگر بیافتد (یا به طور تصادفی یا با قصد قبلی)، سپس با استفاده ازآن می تواند به راحتی وارد حریم خصوصی شما شده و آن را در معرض خطر قرار دهد. برخی از برنامه های کاربردی تا حدودی امنیت حریم خصوصی را برقرار می کنند . اما بسیاری از برنامه های کاربردی با استفاده از روش های ساده و یا روش نسبتا مبهم برای ذخیره سازی اطلاعات استفاده می کنند ، که با این کار براحتی حریم خصوصی شما در معرض خطر قرار می گیرد. به عنوان مثال هر نرم افزار جاسوسی بر روی سیستم شما به راحتی می تواند به کشف این اسراربپردازد. مانند فردی که به سیستم شما دسترسی کامل دارد.

در این مقاله قصد داریم به نقاط روشنی در این مناطق تاریک که توسط بسیاری از برنامه های محبوب به افشای محل ذخیره سازی و مکانیزم رمزگذاری می پردازند اشاره کنیم .در این جا ابتدا اشاره ای می کنیم به چگونگی استفاده از این ابزارها برای کشف کلمات عبور و در بخش آخر به نحوه بازیابی رمزهای عبور ذخیره شده توسط این برنامه های کاربردی خواهیم پرداخت.

در اینجا لیستی از برنامه های محبوب ، که ما کاربران اینترنتی که از آنها ، برای وارد شدن به وب سایتهای مختلف حسابهای کاربری و تالارهای گفتگو و ... استفاده می کنیم درمی یابیم که چگونه اسرار رمز عبور ما را در معرض خطر قرار می دهند . ابتدا در این بخش(یک) به معرفی مرورگرهای اینترنتی و در بخشهای دیگر (بخش دو) به معرفی مسنجرها می پردازیم.

مرورگرهای اینترنتی (Internet Browsers)

Avant

مرورگر آوانت که به سرعت در حال رشد کردن و همه گیر شدن است . که با آوردن سطح جدیدی از شفافیت و کارایی به تجربه مرورگری خود می پردازد.

این مرورگر تمام کلمه های عبور ورود به سیستم وب ها را در فایلی به نام "forms.dat" ذخیره می کند.

مسیرهای ذخیره این فایل در نسخه های مختلف windows به شرح زیر می باشد:

[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Avant Profiles \.default\formdata

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Roaming\Avant Profiles\.default\formdata

Log ها و کلمات رمز عبور وارد شده از طریق این مروگر با فرمت 32 بیتی در یک فایل بنام forms.dat.vdt ذخیره شده اند.مطلب مهم این است که با استفاده از یک الگوریتم ناشناخته با فرمت base64 رمزگذاری و ذخیره می شوند.

Comodo Dragon :

Comodo Dragon مرورگر اینترنت سریع و همه کاره بر مبنای کروم است که دارای سطح بالاتری از امنیت و حریم خصوصی نسبت به کروم می باشد.

این مرورگر تمام کلمه های عبور و ورود به سیستم وب ها را در فایل پایگاه داده ای SQLite به نام " Login Data" در محل های زیر ذخیره می کند:

[Windows XP]
C:\Documents and Settings\<user_name>\Local Settings\Application Data\Comodo\Dragon\User Data\Default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Local\Comodo\Dragon\User Data\Default

با استفاده از ذخیره سازی با فرمت و مکانیزم رمزگذاری با عنوان مرورگر گوگل کروم شما می توانید از COMODO Decryptor رمز عبور را به طور خودکار بازیابی و از همه رمزهای ورود ذخیره شده توسط مرورگر comodo dragon استفاده کنید.

: CoolNovo (formerly ChromePlus)

CoolNovo (که قبلا Chrome Plus) یک مرورگر کرومی مبتنی بر وب می باشد. این مرورگرتمام کلمه های عبور ورود به سیستم وب را در فایل پایگاه داده SQLite به نام" Login Data "محل های زیر ذخیره می کند:

[Windows XP]
C:\Documents and Settings\<user_name>\Local Settings\Application Data\Comodo\Dragon\User Data\Default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Local\Comodo\Dragon\User Data\Default

این ذخیره سازی با استفاده از فرمت و مکانیزم رمزگذاری با مدل گوگل کروم است شما می توانید با ابزار CoolNovo Decryptor رمز عبور به طور خودکار بازیابی همه رمزهای ورود ذخیره شده توسط مرورگر CoolNovoاستفاده کنید.

: Firefox

مرورگر فایرفاکس تا نسخه 3.5 و قبل از آن کلمات عبور و ورود به سیستم را درفایلی بنام " signons.txt" ذخیره می کردند . از نسخه 3.5 به بعد فایرفاکس شروع به ذخیره سازی کلمات عبور در فایل پایگاه داده ای SQLite به نام 'signons.sqlite' را نمود .کلمات عبور ذخیره شده در این جا بر روی فایل ها با استفاده از مدل رمزگذاری DES و به دنبال آن از مکانیزم رمزگذاری base64 برای رمزگذاری ها استفاده می نمودند.

مسیر های زیر محل پیش فرض دایرکتوری پروفایل فایرفاکس است،

[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Mozilla\Firefox\Profiles\<random_name>.default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\AppData\Roaming\Mozilla\Firefox\Profiles\<random_name>.default

شما می توانید برای بازیابی همه این رمزهای عبور از ابزارهایی از قبیل FirePassword (خط فرمان) و یا FirePasswordViewer (GUI) استفاده کنید.

فایرفاکس برای حفاظت بیشتر از کلمات عبور از گزینه اضافی به نام 'master password' برای جلوگیری از کشف این کلمات عبور توسط کاربران مخرب استفاده می کند . جای دیگری که کدهای هش شده و دیگر اطلاعات مربوطه ذخیره می شوند درفایلی بنام " key3.db "در فهرست پروفایل می باشد.

: Flock

مرورگر flock از ذخیره سازی با فرمت مشابه و مکانیزم رمزگذاری در گوگل کروم استفاده می کند. این مرور گر کلمات عبور ورود به سیستم وب سایت ها را در فایل پایگاه داده SQLite به "نام Login Data" ذخیره می کند. محل ذخیره این فایل در نسخه های مختلف windose بشرح زیر می باشد

[Windows XP]
C:\Documents and Settings\<user_name>\Local Settings\Application Data\Flock\User Data\Default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Local\Flock\User Data\Default

تمامی نشانه ها درهنگام ورود ذخیره شده که شامل URL وب سایتها ، شناسه (شماره) زمینه، نام کاربری، نام کاربری و رمز عبور شناسه (شماره) زمینه و رمز عبور رمزگذاری می شود.

شما می توانید از ابزار ChromePasswordDecryptor را برای بازیابی کلمات عبور وب سایت ها در مرورگر Flock استفاده کنید.

: Google Chrome

گوگل کروم تمام ثبت ، نام کلمه عبور را در فایل پایگاه داده SQLite به نام 'Web Data'در داخل دایرکتوری مشخصات ذخیره می کند . نسخه جدیدتر با استفاده از فایل" Login Data " برای ذخیره سازی کلمات عبور ورود به سیستم اقدام به ذخیره سازی آنها می کند.محل ذخیره سازی فایل ها به شرح زیر می باشد

[Windows XP]
C:\Documents and Settings\<user_name>\Local Settings\Application Data\Google\Chrome\User Data\Default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Local\Google\Chrome\User Data\Default

تمامی نشانه ها درهنگام ورود ذخیره شده که شامل URL وب سایت، شناسه (شماره) زمینه، نام کاربری، نام کاربری و رمز عبور شناسه (شماره) زمینه و رمز عبور رمزگذاری می شود.

شما می توانید از ابزار ChromePasswordDecryptor به طور خودکار همه نشانه های موجود بر روی کلمات عبور ذخیره شده توسط کروم را بازیابی و استفاده کنید.

Google Chrome Canary or SXS :

Google Chrome Canary یا SXS نسخه آزمایشی موازی با کروم است .همانند کروم تمام ثبت ، نام کلمه عبور را در فایل پایگاه داده SQLite به نام 'Web Data'در داخل دایرکتوری مشخصات ذخیره می کند. نسخه جدیدتر با استفاده از فایل Login Data برای ذخیره سازی کلمات عبور ورود به سیستم اقدام به ذخیره سازی آنها می کند.محل ذخیره سازی این فایل ها به شرح زیر می باشد

[Windows XP]
C:\Documents and Settings\<user_name>\Local Settings\Application Data\Google\Chrome SXS\User Data\Default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\Local\Google\Chrome SXS\User Data\Default

همچنین از همان ذخیره سازی و مکانیزم رمزگذاری در کروم می توان استفاده کرد .تمام نشانه ها در ورود ذخیره شده که به طور کلی شامل URL وب سایت، شناسه (شماره) زمینه، نام کاربری، نام کاربری و رمز عبور شناسه (شماره) زمینه و رمز عبور رمزگذاری شده است.

Internet Explorer:

اینترنت اکسپلورر مرورگری است که شامل دو نوع کلمه عبور، ثبت نام و احراز هویت HTTP (به طور کلی پروکسی، پیکربندی روتر) است . اینترنت اکسپلورر نسخه پائین تر از 7 هر دو هنگام وارد شدن از طریق HTTP و کلمه عبور تأیید هویت در محل امن شناخته شده ای به نام 'Protected Storage'در محل زیر در رجیستری می باشد

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

در نسخه 7 به بعد اینترنت اکسپلورر با استفاده از مکانیزم جدید برای ذخیره سازی هنگام وارد شدن با کلمه عبور و رمز عبور را برای هر وب سایت همراه با هش URL وب سایت رمز گذاری کرده و در محل زیر در رجیستری ذخیره می کند

HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\IntelliForms\Storage2

همچنین اینترنت اکسپلورر 7 به بعد، کلمه عبور از طریق HTTP مورد تأیید هویت در 'Credentials store' بر اساس نسخه سیستم عامل در مسیرهای زیر ذخیره می شود.

[Windows XP]
C:\Documents and Settings\[username]\Application Data\Microsoft\Credentials

[Windows Vista/Windows 7/Windows 8]
C:\Users\[username]\AppData\Roaming\Microsoft\Credentials

: Maxthon

ماکستون (نسخه 3.1.7.1000) مرورگری است وقتی که کاربران وارد حساب کاربری در تمام وب سایتها می شوند کلمات عبور را در فایلی بنام "MagicFill2.dat" در مسیر زیر ذخیره می کند.

[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Maxthon3\Users\<user_name>\MagicFill

[Windows Vista/Windows 7/Windows 8]
C:\Users\Administrator\AppData\Roaming\Maxthon3\Users\<user_name>\MagicFill

توضیح اینکه با الگوریتم ناشناخته ای رمز گذاری می شود.

: Opera

اپرا مرورگری است که رمز عبور ورود به سیستم را در یک قالب رمزگذاری 'Magic Wand File' که به آن فایل " Wand.dat " گفته می شود در داخل دایرکتوری ذخیره می کند . همانطور که در زیر نشان داده شده است. مشخصات این مسیر برای نسخه های مختلف از اپرا متفاوت است

For Opera Version 10 and above
[Windows NT/2K/2k3/XP]
C:\Documents and Settings\<username>\Application Data\Opera\Opera\wand.dat

[Windows Vista/Windows 7/Windows 8]
C:\users\<username>\AppData\Roaming\Opera\Opera\wand.dat

For Opera Version less than 10
[Windows NT/2K/2k3/XP]
C:\Documents and Settings\<username>\Application Data\Opera\Opera\profile\wand.dat

[Windows Vista/Windows 7/Windows 8]
C:\users\<username>\AppData\Roaming\Opera\Opera\profile\wand.dat

این فایل ها به طور عمده شامل URL وب سایت، نام کاربری و رمز عبور اطلاعات است که با استفاده از الگوریتم DES رمزگذاری شده است.

Safari:

این مرورگر با استفاده از فرمت ذخیره سازی قوی و مکانیزم رمزگذاری برای ذخیره سازی کلمات عبور ورود به وب سایت استفاده می کند . ورود رمز عبور به همراه دیگر اطلاعات درفایلی بنام " keychain.plist "در محل زیر ذخیره می شود.

[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Apple Computer\Preferences

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\Appdata\AppData\Roaming\Apple Computer\Preferences

این فایل از منابعی مانند Keychain برای استفاده از فرمت باینری با استفاده از فهرست مالکیت (به طور معمول در MAC) که حاوی اطلاعاتی مانند وب سایت نام سرور، ورود کاربر نام کاربری و رمز عبور رمزگذاری شده است. رمز عبور با استفاده از توابع رمزنگاری با ارزش نگه داشته می شود .

SeaMonkey:

این مرورگر وب ، مبتنی بر اینترنت موزیلا است. برای رمز عبور از همان فرمت ذخیره سازی و مکانیزم رمزگذاری در مرورگر فایرفاکس استفاده می کند.این مرورگر مشخصات کاربر از جمله ذخیره کردن کلمه عبورهنگام ورود به سیستم را در فایلی به نام "signons.sqlite" در مسیر زیر ذخیره می کند.

[Windows XP]
C:\Documents and Settings\<user_name>\Application Data\Mozilla\SeaMonkey\Profiles\<random_name>.default

[Windows Vista/Windows 7/Windows 8]
C:\Users\<user_name>\AppData\Roaming\Mozilla\SeaMonkey\Profiles\<random_name>.default

همانطور که گفته شد این مرورگر از فرمت و مکانیزم رمزگذاری در فایرفاکس استفاده می کند.

پایان بخش اول

پیروز و موفق باشید.

X3N0N & F4RY4R_RED