アンラボ・セキュリティレター

Press Ahn

2017.8　Vol.44

自動ログインの利便性と、そのリスク

THREAT ANALYSIS・IDENTITY THEFT

自動ログインの利便性と、そのリスク

最新の統計によると、1人当たり平均 3つのソーシャルメディアを利用しているという。また使用中のメールアカウントも 3つ以上が最も多かった。このように複数のアカウントを利用するうえでそれぞれの IDやパスワードを記憶することや、頻繁に利用するサービスに毎回ログインすることが面倒だと感じるユーザーも多いはず。だからこそ多くのユーザーは「自動ログイン」機能を利用している。だが本機能を利用する際にセキュリティリスクが高まる点を忘れてはならない。今回のコラムでは、自動ログイン機能を利用して個人情報を盗むマルウェアについて紹介する。

マルウェアの作成者らは金銭的な利益を得るため、さまざまな手法を駆使する。最近はデータを人質に身代金を要求するランサムウェアが多くなったが、オーソドックスな手法も依然存在している。代表的なケースは、ユーザーのログイン情報を盗むマルウェアだ。直近、ブラウザ、メールクライアントを対象にログイン情報を盗むマルウェアが相次いで発見されている。マルウェアの主な感染経路は、一般的なマルウェア同様「メール」である。ほとんどはスパムメールから大量に配布されるが、一部特定の対象を狙った標的型攻撃の様相を見せることもある。

ログイン情報横取り

攻撃者がログイン情報を盗む手法は大きく 2つある。ユーザーが入力したキーの値を横取りしたり、システムに保存されたログイン情報を盗む方法だ。

1. キー入力情報を横取りする

有名なサービスプログラムの画面を装ってユーザーにログイン情報を入力するように仕向けたり、キーロガー(key-logger)を利用してユーザーのアカウント情報を盗む手法だ。だがこの手法にはユーザーが直接入力する情報のみ横取りできるという限界がある。

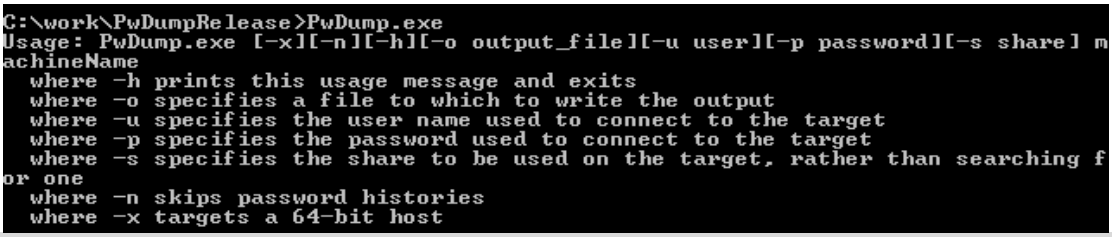
[図1] PayPalを装ったフィッシングプログラム

2. 保管されたログイン情報を盗む

アプリケーションの自動ログイン機能を使用すると、ユーザーが初回入力したアカウント情報がファイルまたはデータベースの形でどこかに暗号化されて保存される。しかし一部では暗号化方式ではなくエンコードでやパスワードをそのまま平文形式で保存したりする。こうなると攻撃者が目的とする情報の保管場所さえ事前に把握していれば、簡単にログイン情報を盗むことができる。

パスワード復元プログラムと自動ログインの脆弱性

ユーザーが忘れてしまったパスワードを探すために使用する「パスワード復元プログラム」を利用する場合もある。パスワード復元プログラムは、アカウント情報を忘れてしまったユーザーが利用するプログラムだ。問題はパスワードの復元原理が解析され、攻撃者がログイン情報を盗むマルウェアを作るために活用することだろう。代表的なものとしては Windowsのログイン情報を確認する「Pwdump」というプログラムがある。これはセキュリティアカウントマネージャー(SAM)のローカルユーザーアカウントのパスワードハッシュ値を出力するプログラムだ。
攻撃者がハッシュ値を入手すれば、ログインに必要な情報を把握して攻撃対象のシステムを掌握できる。



[図2] Pwdump実行画面

このほかブラウザのログインパスワードを表示するプログラムがあるが、これもまた忘れてしまったパスワードを探すためのプログラムだ。攻撃者はこれらのプログラムを利用してユーザー情報を入手することができる。

[図3] 実際のハッキングに悪用されたブラウザのパスワード復元プログラム

1.攻撃対象

プログラムごとにログイン情報を保管する位置と方法が異なるため、攻撃者は盗もうとするプログラムを分析してログイン情報の保管位置を調べた後で情報にアクセスする。主にログイン情報奪取の対象となるプログラムは、以下の通りだ。

分類	プログラム名
メールクライアント	Foxmail, Gmail Notifier, IncrediMail, Outlook, ThunderBird, Windows Live Mail
FTPクライアント	Alftp, Dreamweaver, FileZilla, FlashFXP, FTPCommander, SmartFTP, WS_FTP
ブラウザ	Avant, Chrome, Chrome Canary or SXS, Comodo Dragon, CoolNovo, Firefox, Flock, Internet Explorer, Maxthon, Opera, Safari, SeaMonkey
メッセンジャー	AIM(AOL Instant Messenger), Beyluxe Messenger, BigAnt Messenger, Camfrog Video Messenger, Digsby IM, Google Talk(GTalk), IMVU Messenger, Meebo Notifier, Miranda, MSN Messenger, MySpaceIM, Nimbuzz Messenger, PaltalkScene, Pidgin, Skype, Tencent QQ, Trillian, Windows Live Messenger, XFire, Yahoo Messenger
その他	Google Desktop Search, Heroes of Newerth, Internet Download Manager(IDM), JDownloader, Orbit Downloader, Picasa, RemoteDesktop, Seesmic, SuperPutty, TweetDeck

[表1] 主な攻撃対象

2.ログイン情報の保管場所

ユーザーが保存したログイン情報は、ファイルやレジストリに暗号化されて格納されることもあるが、平文や簡単なエンコード形式で保存される場合もある。ログイン情報の保管位置は次のサイトで確認できる。(英)http://securityxploded.com/passwordsecrets.php

■ Internet Explorer

IEは、ログイン情報をレジストリに保存する。

HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Explorer¥IntelliForms¥Storage2

■ Chrome

Chromeは「Login Data」ファイルにログイン情報を保存する。

C:¥Users¥<user_name>¥Appdata¥Local¥Google¥Chrome¥UserData¥Default¥Login Data

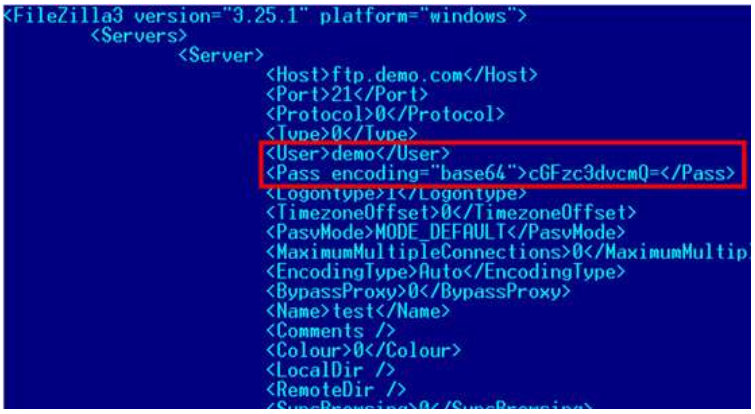
■ Outlook

Outlookは、レジストリにログイン情報を暗号化して保存する。

HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥(バージョン)¥Outlook¥Profiles¥Outlook

■ Filezilla

代表的なファイル送信プロトコル(File Transfer Protocol、FTP)プログラム「Filezilla」は、ログイン情報を sitemanager.xmlなどのテキストファイルとして保存する。もとは平文のまま保管したが、今は Base64でエンコードされ Base64デコーダによって簡単にパスワードを確認できる。



[図4] Filezillaのログインパスワードを保存する

[図5] Base64変換結果

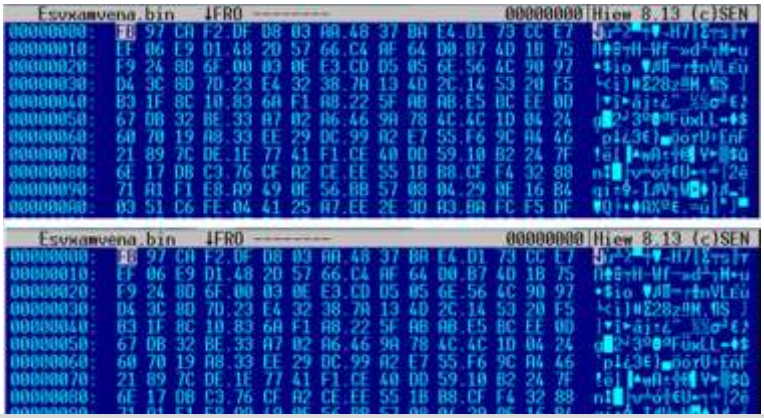
パスワードに使用された値を Base64でにデコードすると、[図5]のように「password」というパスワードを確認できる。

3. ログイン情報掠取りタイプのマルウェア

システムに保管されたログイン情報を盗む代表的なマルウェアは次の通りだ。

■Decoloader（Tkhawk.exe）

RAR SFX(Self-Extractor)ファイルで、ファイル内に実行ファイルと暗号化されたデータファイルが存在する。ファイル名 Esvxamvena.binと、Fbulmigrmkwhr.binは暗号化されたデータファイルである。



[図6] 暗号化されたデータファイル

Osslpjuy.exeは「.NET」で作成されたファイルだが、実行されると.NET関連ファイルの「RegAsm.exe」が実行されて終了する。RegAsm.exeのメモリをみると、コードが Private属性で実行されることが分かる。

ase address	Type	Size	Protect...	Use
0x1c0000	Private	64 kB	NA	
0x1d0000	Private	64 kB	NA	
0x1e0000	Private	64 kB	NA	
0x1f0000	Private	256 kB	RWX	Heap 32-bit (ID 3)
0x230000	Private	64 kB	NA	
0x240000	Mapped	4 kB	RW	
0x250000	Private	1,024 kB	RW	Stack 32-bit (thread 3464)
0x350000	Private	64 kB	NA	
0x360000	Mapped	12 kB	R	C:₩Windows₩SysWOW64₩l_intl.nls
0x370000	Mapped	4 kB	R	
0x380000	Mapped	68 kB	R	C:₩Windows₩System32₩C_1252.NLS
0x3a0000	Private	64 kB	RW	Heap 32-bit (ID 6)
0x3b0000	Private	64 kB	RW	
0x3c0000	Private	64 kB	NA	
0x3d0000	Mapped	20 kB	R	C:₩Windows₩assembly₩GAC_32₩mscorlib₩2.0.0.0__b77a5c561934e089₩sorttbls.n
0x3e0000	Private	64 kB	NA	
0x3f0000	Mapped	8 kB	R	
0x400000	Private	544 kB	RWX	

[図7] RegAsm.exe内メモリ

[図7]の 0x1f0000アドレスをみると次のような疑わしい文字列を確認できる。

C:¥Users¥Jovan¥Documents¥VisualStudio2010¥Projects¥Stealer¥CMemoryExecute¥CemoryExecute¥obj¥Release¥CMemoryExecute.pdb

[図8] マルウェアの特徴的な PDB情報

メモリには他の実行ファイルも存在するが、これらはブラウザのログイン情報を確認する WebBrowserPassViewとメールのログイン情報を知る Mail PassViewである。同マルウェアは従来のパスワード復元プログラムを、こっそり実行してログイン情報を取得した後で流出する。

■Trojan/Win32.Loginstealer（fontwow64.exe）

Trojan/Win32.Loginstealerと診断されたfontwow64.exeは、2017年3月に発見されたログイン情報を盗むマルウェアであり、関連する変種は2015年10月にも発見された。これらのサンプルは双方ともに、まだVirus Totalなどのマルウェアスキャンサービスにアップロードされていない。大量のメールによる拡散よりは標的型攻撃に利用された可能性がある。同マルウェアが実行されると、暗号化されたUsernameとPasswordのパスワードを解いてログイン情報を盗む関数を実行する。主な文字列は、暗号化され保存されている。

```
SetErrorMode(0x8007u);
memset(&v5, 0, 0x528u);
v12 = Username_49E688;
v13 = 0;
v10 = Password_49E694;
v11 = 0;
v5 = -1;
v6 = 0i64;
v7 = 0;
v8 = 0i64;
v9 = 0;
decode_447B90(&v6, (const char *)&v12);       // Username
decode_447B90(&v8, (const char *)&v10);       // Password
StealLogin_447540((int)&v5);
return 0;
```

[図9] Trojan/Win32.Loginstealerコードの先頭

保存されたログイン情報を盗む関数が実行されると、drf2EPOREVHN.jpg、drf2EPOREXKK.jpgなどの任意の名前とJPG拡張子を持つファイルを作成する。以後、様々なブラウザ、メッセンジャー、メールクライアントなどのログイン情報を収集して保存する。

```
if ( CreateJPG_447710(v1) )                   // %temp%\random.jpg (drf2EPOREVHN.jpg)
{
  Steal_FoxMail_44B2C0((int)v1);              // AeroFox\Foxmail\Preview
                                              // Netease\FlashMail
                                              // IncrediMail
                                              // OperaMail.exe
                                              // Google Desktop\Mailboxes
                                              // Google Talk\Accounts
                                              // Internet Explorer
                                              // Chrome
                                              // Mozilla Firefox
                                              // Safari
                                              // Windows Mail
                                              // Outlook 11.0 - 15.0
                                              //
                                              //
  Steal_FlashMail_4A0A80((int)v1);
  Steal_IncrediMail_44E610((int)v1);
  Steal_OperaMail_4AFC10((int)v1);
```

[図10] ログイン情報を収集

盗まれたログイン情報、APT攻撃に使用される可能性も

攻撃者は盗んだログイン情報を利用してユーザーのメールやコミュニティ活動の履歴を覗き見できる。先日メールアカウント情報をハッキングされたユーザーが、さらにメールボックスに保管しておいた個人情報履歴を盗まれたケースがあった。盗まれたログイン情報は第二次三次攻撃に利用されることもあるので、ユーザーのログイン情報は狙われやすいのだ。

企業でこれらの悪質なマルウェアが継続的に発見される場合、ターゲット攻撃や、標的型攻撃(APT)を成就させるための下準備である可能性もあり、厳重な注意が求められる。実際に米国の政治団体への攻撃にもログイン情報の横取りマルウェアが使用されていたことが分かった。

ログイン情報を横取りするマルウェアに感染していた場合は、周期的なパスワード変更も用無しになってしまう。これらのマルウェアによる被害を減らすためには自動ログイン機能をなるべく使用しないことが望ましい。幸いなのは、保存されたログイン情報を流出するパターンは決まっているという点だ。もしもあるプログラムからログイン情報の保管位置にアクセスする場合「ログイン情報を盗むマルウェア」と判断することができる。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)