アンラボ・セキュリティレター

Press Ahn

2022.9　Vol.105

ハッカーが自動ログイン機能を好む理由

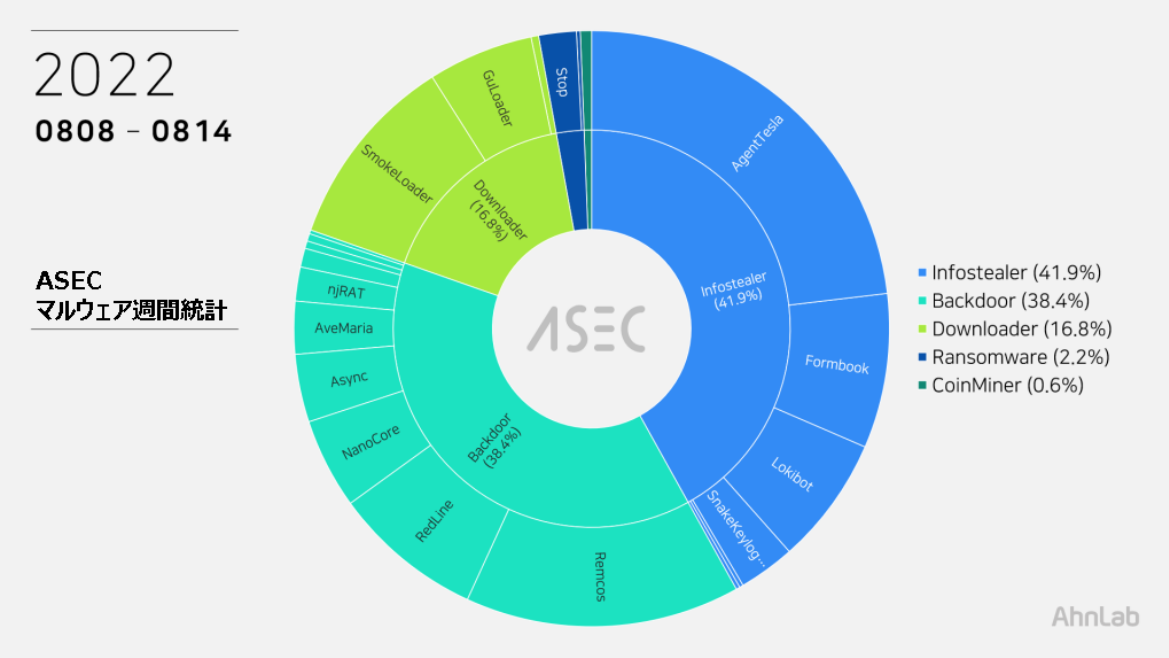
ハッカーが自動ログイン機能を好む理由

近年流行しているマルウェアを語る上で、必ずと言ってよいほど登場するのが「インフォスティーラー（InfoStealer)」だ。インフォスティーラーは文字通り、ユーザーの様々な情報を狙う情報窃取型マルウェアのことである。特に、Web サイトやプログラムの「自動ログイン」機能を使用している場合、インフォスティーラーに感染すると、複数のサービスアカウントの資格証明を奪取されてしまう。一般のユーザーは通常、同一アカウントおよびパスワードを用い、多数のサービスを利用しているため、その危険性が非常に高いと言えるだろう。

今回は、自動ログインを使用する被害者側が、インフォスティーラーによって情報を奪取される原理と、これによる被害を最小限に抑える方法を紹介する。

インフォスティーラー（InfoStealer）は、OS やプログラムに保存されている資格証明、および各種情報を盗み出すマルウェアである。一般的に、実行されると各種情報を自動で収集し、流出させるタイプのマルウェアを意味する。

インフォスティーラーは、攻撃頻度数が増加の一途をたどり、その種類や奪取情報も多様化している。アンラボが自社の ASEC ブログにて毎週公開している「ASEC マルウェア週間統計」でも、相当な長期間にわたり、インフォスティーラーが 1位を占めている。



[図1] 8月 2週目のマルウェア週間統計

インフォスティーラー型のマルウェアは、様々な形でユーザーの情報を奪取するが、今回はプログラム、特に Web ブラウザの自動ログイン機能を使用中の状況で、情報が流出する原理を説明していく。

基本概念

ユーザーがプログラムの「自動ログイン」機能を使用している場合、資格証明情報は通常、ファイルまたはデータベース形式に暗号化した状態で保存されている。一部のプログラムでは暗号化方式ではなく、エンコード、さらには平文形式で保存されることもある。暗号化方式に関しても、比較的簡単に破られることが多いため、攻撃者が奪取を目的としたプログラム暗号情報の保存場所やアルゴリズムを把握していれば、資格証明情報の窃取はそう難しくない。

攻撃者らが情報奪取を行う手口としては、大きく ▲パスワード復元プログラムの利用、▲マルウェア内の情報流出機能の活用、この 2つのタイプに分けることができる。

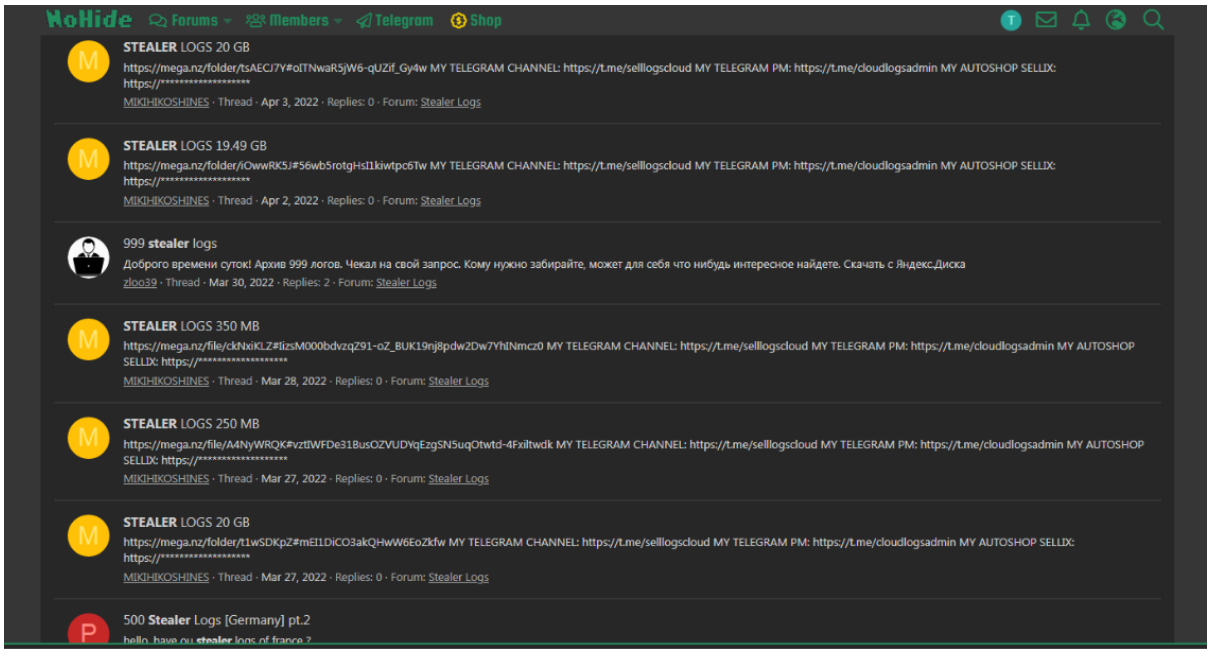
パスワード復元プログラムとは、Windows や Web ブラウザのログインパスワードを忘れた際、ユーザーが利用するプログラムのことである。攻撃者側も、パスワード情報を入手するためにこのプログラムを活用する。パスワード復元プログラムをそのまま使用することもあるが、メモリから実行することでユーザー情報を不明にするケースも多発している。

マルウェア内の情報流出機能は比較的広く知られており、インターネットバンキングの情報流出型や、バックドア型などのマルウェアに機能として含まれている場合もある。中でも、DarkCrystal (ダーククリスタル)、Formbook (フォームブック)、XLoader (エクスローダ) などが、情報流出機能を持つ代表的なマルウェアとして挙げられる。

インフォスティーラーはなぜ脅威とされるのか？

インフォスティーラー型のマルウェアにおける最大の問題点とは何か。攻撃者は、インフォスティーラーを用いて、プログラムに保存されている資格情報を根こそぎ奪取する。そのため、ユーザーが使用中のパスワードをいくつか分析するだけで、他のサイトのパスワードや、今後使用するであろうパスワードまでも予想できてしまう。つまり、2次被害を引き起こす可能性が高いのだ。

また、単にユーザーのログイン情報、クレジットカード番号情報などを奪取するだけに留まらず、収集した情報を組織内への侵入時に活用することもある。インフォスティーラーを用いて収集された情報が、ダークウェブ（Dark Web）上に公開・販売されるケースもあり、攻撃者は特定の企業や組織の資格情報をダウンロード、もしくは購入し、攻撃時に悪用する。



[図2] ダークウェブ上に公開された資格証明情報

最近では、サイバー犯罪組織だけでなく、背後に国家支援を受けているとされる脅威グループも、インフォスティーラー型のマルウェアを頻繁に利用している。代表的な例として、2020年 10月、北朝鮮の支援を受けたと推定される「アンダリエル（Andariel）」グループのインフォスティーラー型マルウェアが発見された。このマルウェアは、Chrome、Firefox、Internet Explorer などの Web ブラウザに保存されているログイン情報を奪取するものだ。

今まで攻撃者が奪取の対象としていた情報は、システム情報や各種プログラムのログイン情報であった。しかし、ここ最近は、仮想通貨のウォレット情報やゲームなど、その範囲が徐々に拡大しつつある。一方で、2018年以降に使用率が急激に減少した Internet Explorer を、対象プログラムから外したマルウェアが増加している。攻撃者側も、最大限の利益を得るために、トレンドに合わせて攻撃手法を進化させているのだ。

インフォスティーラーは、他のマルウェアと同様に、メール・Web サイトへのアクセス・プログラムのダウンロードなどから感染する。攻撃者は、クラック（Crack）、シリアルキー生成・取得 プログラム（Keygen）、KMS（Key Management Service）などにマルウェアを仕込み流布する場合が多い。特に、KMS 認証プログラムは、家庭だけでなく大企業でも広く使用されており、マルウェア製作者が流布方法として多く用いている。

また、コロナ禍によるテレワークの拡大に伴い、個人 PC 、または家族共用 PC を業務に用いることも増えた。この際、業務に必要なプログラムをライセンスなしで使おうと、クラックなどをダウンロードしたことで、インフォスティーラーに感染する事例も度々発生した。稀なケースではあるが、サプライチェーン攻撃の事例も確認されている。

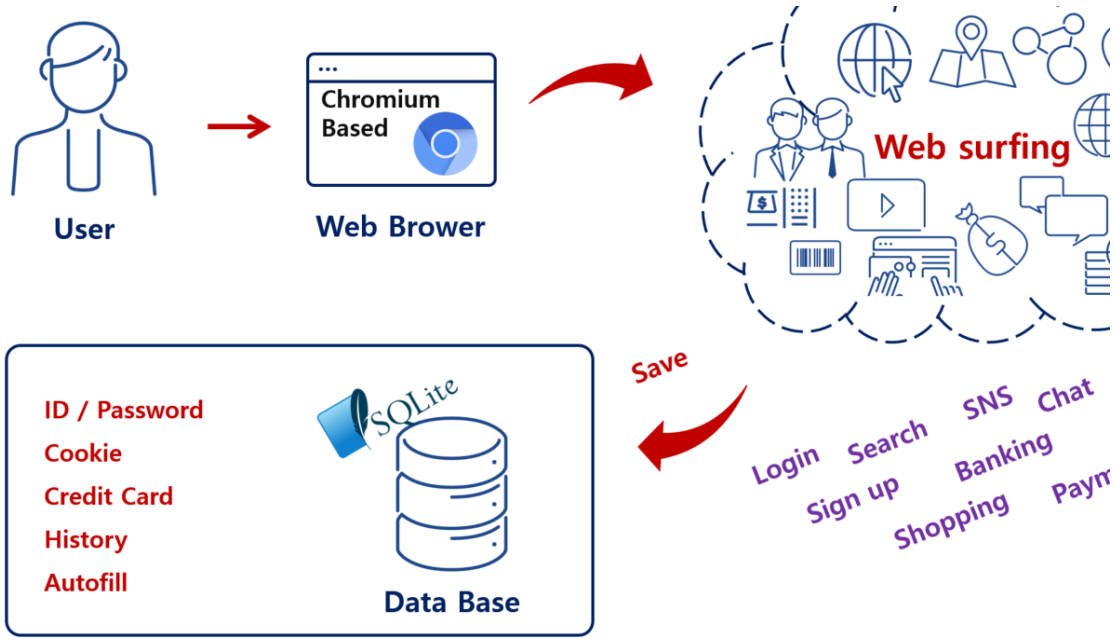
「自動ログイン」機能使用時の情報奪取原理

冒頭にて、プログラムおよび Web ブラウザの自動ログイン機能を使用している場合、インフォスティーラー型マルウェアを用いた情報奪取が容易であると述べた。その理由は何か？複数の関連事例のうち、ユーザーの身近で起こりうる Web ブラウザの保存情報に関する流出原理を見てみよう。

1. Chromiumベースのブラウザ

Chromium（クロミウム）は、Google によって開発・管理されているオープンソースの Web ブラウザで、現在最も使用率の高いブラウザエンジンだ。代表的なものとして、Chrome、Edge、Opera などが Chromium コードをベースに開発された。

Chromium ベースの Web ブラウザは、ユーザーがネットサーフィンを行う際に保存する、アカウント（ID・パスワード）情報・Cookie（クッキー）データ・カード情報・履歴・オートフィル（Autofill：自動入力）などを、ローカルシステムである SQLite の DB ファイルに保存する特徴を持つ。



[図3] ブラウザ内の保存内容

SQLite の DBファイル内にある一部の機密データは、AES（Advanced Encryption Standard：高度暗号化標準）によって暗号化された状態で管理される。Chromium の暗号化データ管理は、ローカルシステムのユーザーだけが情報を復号化することができ、DataProtection API によって暗号化された AES キーを、DPAPI blob 形態で保存する。このデータは Base64 エンコードの状態で、(省略) …¥User Data¥Local State JSON ファイルの "os_crypt" : {"encrypted_key"} 位置に保存されている。

インフォスティーラーは、アカウント・Cookie・カード・履歴・オートフィル情報が保存された DB ファイルを対象に、SQL クエリ（query）を介して必要なデータを抽出する。さらに、AES キーを復号化することで、暗号化データの平文情報を収集することが可能だ。

名前	パス	テーブル	暗号化
アカウント(ID/Password)	%LocalAppData%¥Google¥Chrome¥User Data¥Default¥Login Data	logins	O
クッキー(Cookies)	%LocalAppData%¥Google¥Chrome¥User Data¥Default¥Network¥Cookies	cookies	O
カード(Card)	%LocalAppData%¥Google¥Chrome¥User Data¥Default¥Web Data	credit_cards	O
履歴(History)	%LocalAppData%¥Google¥Chrome¥User Data¥Default¥History	urls	X
オートフィル(Autofill)	%LocalAppData%¥Google¥Chrome¥User Data¥Default¥Web Data	autofil	X

[表1] Chromium に保存されている主なデータファイル

名前	対象ファイル	SQL Query
アカウント (ID/Password)	Login Data	SELECT origin_url, username_value, password_value FROM logins
クッキー	Network¥Cookies	SELECT host_key, name, Path, expires_utc, is_secure, value, encrypted_value FROM cookies
カード	Web Data	SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
履歴	History	SELECT url, title, visit_count, last_visit_time FROM urls
オートフィル	Web Data	SELECT name, value FROM autofill

[表2] Chromium 情報収集時の SQL クエリ

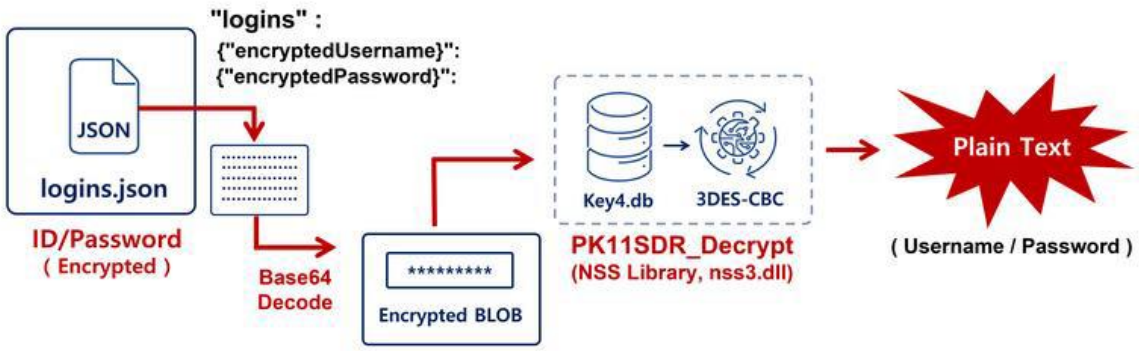
また、パスワード以外に、暗号化された全フィールド値も同様の方法で平文形式に復号化することができる。復号化が可能な情報として、▲Cookies テーブルの encrypted_value、▲Credit_Card テーブルの card_number_encrypted フィールドなどがある。

2. Gecko ベースのブラウザ

Gecko (ゲッコー) とは、Mozilla 財団により開発・管理されているオープンソースの Web ブラウザエンジンである。このエンジンを使用する代表的な Web ブラウザには、Firefox、Thunderbird、IceDragon、Cyberfox などがあり、Chromium に次いで2番目に多く使用される Web ブラウザエンジンだ。

Gecko ベースのブラウザ上に保存されたアカウント情報は、logins.json ファイルに暗号化された状態で格納される。Gecko ブラウザの暗号化データは、Mozilla によって開発された NSS ライブラリの PK11SDR_Encrypt / PK11SDR_Decrypt 関数を利用し管理されている。この関数における内部動作のプロセスをかいつまんで説明すると、key4.db ファイルから Master Key、Salt 値を抽出し、3DES-CBC 演算によって暗号化および復号化される方式だ。

インフォスティーラーは、Gecko ベースのブラウザが使用する nss3.dll の PK11SDR_Decrypt 関数を動的にロードし、logins.json から抽出した暗号化状態のアカウント情報を平文に復号化することができる。



[図4] Gecko ベースの復号化プロセス

Gecko ベースブラウザに関する主要ファイル、およびブラウザ情報収集時の SQL クエリ情報は、それぞれ [表3]、[表4] の通りだ。

名前	パス	暗号化
アカウント (ID/Password)	%AppData%Mozilla¥Firefox¥Profiles¥[ランダム値]¥logins.json JSON	O
クッキー	%AppData%Mozilla¥Firefox¥Profiles¥[ランダム値]¥cookies.sqlite	X
履歴	%AppData%Mozilla¥Firefox¥Profiles¥[ランダム値]¥places.sqlite	X

[表3] Gecko ベースの主なファイル情報

名前	対象ファイル	SQL Query
クッキー	cookies.sqlite	SELECT host, name, path, value, creationTime, expiry, isSecure FROM moz_cookies
履歴	places.sqlite	SELECT url, title, visit_count, last_visit_date FROM moz_places

[表4] Gecko 情報収集時の SQL クエリ

また、Gecko ブラウザの Cookie 情報は cookies.sqlite に、履歴は places.sqlite の DB ファイルに保存される。アカウント以外に関しては、別途暗号化なしに平文で保存されているため、攻撃者が容易に情報を入手することが可能だ。

自動ログインを狙うインフォスティーラー、確かな脅威

Web ブラウザ、またはプログラムの自動ログイン機能を使用している場合、インフォスティーラーにより簡単に情報を奪取される可能性がある。そして、こうした攻撃によるセキュリティ侵害事例は、国内でも実際に発生しているため、一層の警戒心を持たなければならない。

アンラボの ASEC 分析チームは、2021年 12月、某企業の内部ネットワークにおける侵害事例調査で、企業ネットワークのアクセス時に使用された VPN アカウントが、テレワーク中の社員の個人 PC からの流出したことを確認した。被害が発生した企業では、テレワーク中に社内ネットワークにアクセスできるよう、VPN サービスを提供しており、社員は支給されたノート PC、または個人 PC で VPN にアクセスし業務を行っていた。

攻撃元となった社員は、Web ブラウザにて提供されるパスワード管理機能を利用しており、VPN サイトのアカウントおよびパスワードを Web ブラウザに保存して使用していた。こうした状況で、アカウント情報を狙うマルウェアに感染したため、多数のサイトのアカウン

トとパスワードが流出することとなった。その中に企業の VPN アカウントも含まれており、流出した VPN アカウント情報は、約 3ヶ月後に企業内部のネットワークハッキングに悪用されたのである。

被害社員の PC は、家庭内で家族全員が使用しており、安全に管理されていなかったことも判明している。以前から様々なマルウェアに感染しており、他社のワクチンがインストールされていたものの、検知・駆除がきちんと行われていなかった。

さらに、感染したマルウェアの中には、Redline Stealer 系のマルウェアも含まれていた。2020年 3月、ロシアのダークウェブ上に初めて登場した Redline Stealer は、Web ブラウザに保存されたアカウント情報を収集するものだ。この Redline Stealer は、ピッチシフト（音程補正）プログラムである「SoundShifter」のクラックプログラムに偽装し、オンライン上に流布されていた。ユーザーはソフトウェア名、および「crack」、「free」などのキーワードからファイルを検索し、ダウンロードしたファイルを PC 内にインストールしたため、マルウェアに感染したのである。

最も効果的なセキュリティ方法は「予防」

このように、自動ログイン機能を使用すると、インフォスティーラー型マルウェアによるアカウントの情報奪取が一層容易になり、実際に被害事例も発生している。では、こうした情報奪取を最小限に抑えるためにはどうすればよいか？

私達は風邪を引くと、病気を治し、症状を最小限にするために様々な手段をとる。病院に行き診察を受けた後、解熱剤や抗生剤を処方してもらったり、自分で沸かした温かいお茶を飲み、十分な休息をとったりする。こうした対応をとることで、ほとんどの場合は風邪の症状が回復していく。だが根本的に、風邪を引かず健康を維持できるならそれに越したことはない。そのためには、頻繁な手洗いに十分な水分補給など、健康でいるための基本的なことを守りながら生活するのが何よりである。コロナ禍以降、マスクをつけて生活するのもこうした理由からだ。

サイバーセキュリティ、特に今回取り上げた情報流出に関する被害は、上記の風邪の話に通じるものがある。情報の流出後に後続措置を行い、被害を抑えることも大切だが、基本的なセキュリティルールを遵守し、情報奪取を事前に食い止めることが最善策であろう。まず、Web サイトやプログラムを使用する際、できる限りアカウント情報は保存しないことをお勧めする。もちろん便利な機能ではあるが、今回紹介した事例のように、インフォスティーラー型マルウェアに感染すると、いとも簡単に保存情報が流出してしまうため、使用頻度を最小限に抑えるべきである。

また、アンラボだけでなく、他の機関らも普段から強調しているセキュリティルールとして、▲違法ソフトウェアのダウンロードおよび使用、▲信頼できない Web サイトへのアクセス、▲疑わしいメール添付ファイルの実行および URL クリックなどは「自制」しなければならない。さらに、ワクチンなどのセキュリティソフトウェアや、使用中のプログラムが最新バージョンにアップデートされているかどうか、常日頃から確認する必要がある。

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)