AhnLab

安全月刊

2022.09 Vol.118

InfoStealer 恶意代码

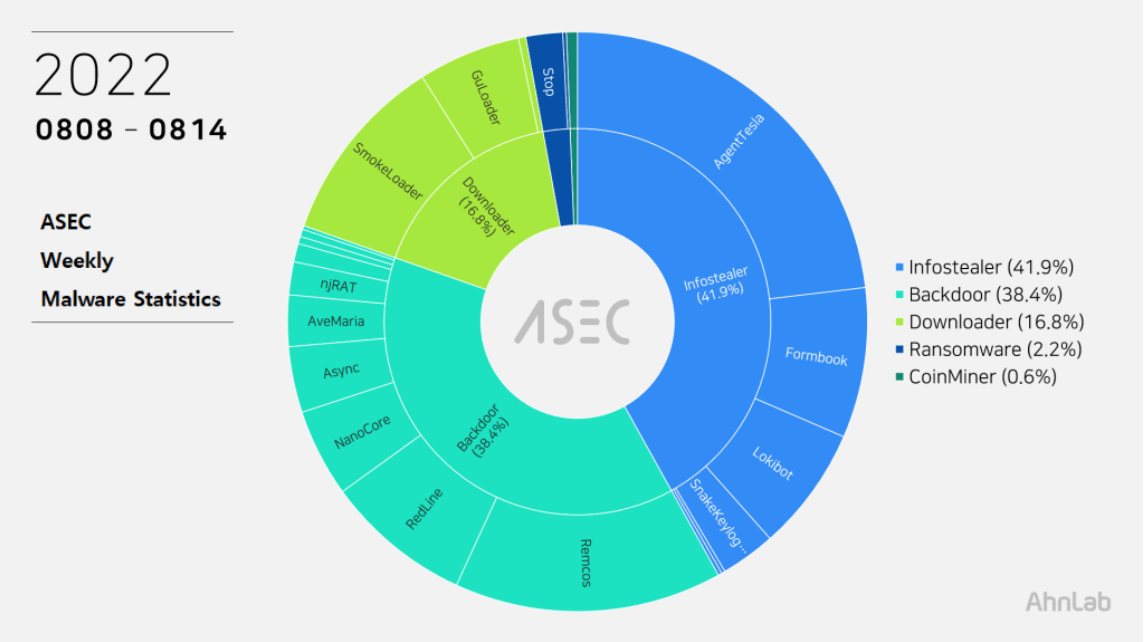
浅谈利用自动登录漏洞的攻击及应对措施

说起近期流行的恶意代码，就不得不提到“InfoStealer”。InfoStealer 从字面上可以看出，是一种窃取用户信息的恶意代码。尤其是，当用户使用网站或程序的“自动登录”功能被 InfoStealer 感染时，会被窃取多个服务帐户的凭证。由于一般用户通常使用相同的帐号和密码使用多个服务，因此信息泄露会造成很大的损失。

在本文中，我们将介绍 InfoStealer 如何利用自动登录漏洞窃取用户信息以及将由此造成的损失降到最低的对策。

InfoStealer 一般指间谍软件，它窃取存储在操作系统或程序中的凭证和各种信息。通常，当恶意代码运行时，它会自动收集各种信息并泄露。

InfoStealer 的攻击更加频繁起来，其类型和窃取的信息也变得更加多样化。在 AhnLab 通过其 ASEC 博客每周发布的“ASEC 每周恶意代码统计”中，InfoStealer 长期以来一直位居榜首。



【图1】8月第2周恶意代码统计

InfoStealer 以各种形式窃取用户信息，本文说明了使用程序（尤其是网页浏览器）的自动登录功能时信息泄露的原理。

基本概念

当用户使用程序的“自动登录”功能时，凭证信息通常被加密并以文件或数据库形式保存。在某些程序中，被编码而不是加密，甚至以纯文本形式保存。在多数情况下，加密方式也比较容易被破解，所以如果攻击者获知要窃取的程序的加密信息保存位置和算法，就可以窃取凭证信息。

攻击者窃取信息的方法大致可分为两种形式：▲使用密码恢复程序、▲恶意代码中包含的信息泄露功能。

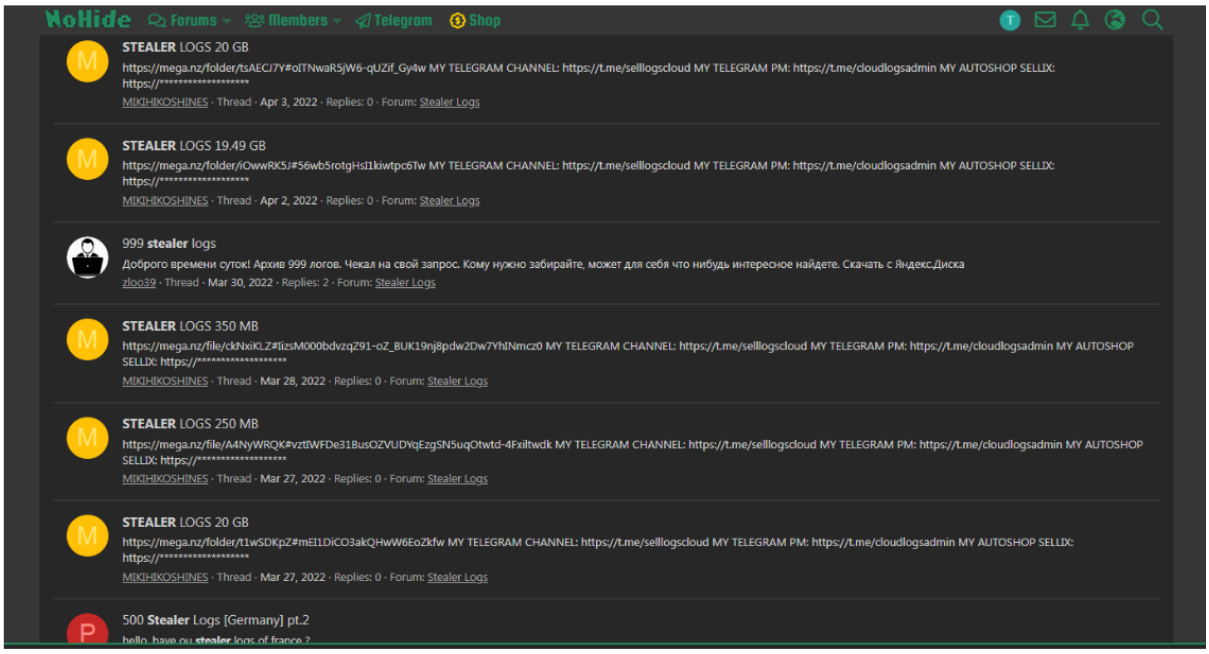
密码恢复程序是用户忘记 Windows 或 Web 浏览器登录密码时可使用的程序。攻击者使用该程序计算密码。在某些情况下，密码恢复程序按原样使用，但在许多情况下，它们在内存中运行，使用户无法察觉到。

恶意代码中的信息泄露功能是众所周知的，网上银行信息泄露恶意代码或后门等恶意代码功能也包括在内。DarkCrystal、Formbook 和 XLoader 等恶意代码通常具有信息泄露功能。

InfoStealer 为何具有威胁性?

InfoStealer 的最大问题是可以分析用户使用的多个密码来推测其他网站的密码或未来的密码，这是因为攻击者窃取程序中存储的所有凭据。简单来讲，这极有可能造成二次损害。

此外，不只是简单地窃取用户登录信息和信用卡号等信息，还可以根据收集到的信息用于渗透组织。使用 InfoStealer 收集的信息有时会在暗网（Dark Web）上公开或出售，攻击者下载或购买特定企业或组织的凭证信息并使用它进行攻击。



【图2】暗网上公开的凭证信息

最近，不仅是网络犯罪组织，疑似受国家资助的威胁组织也在积极地使用 InfoStealer 恶意代码。例如，在2020年10月，发现一种推测由朝鲜资助的 Andariel 组织的 InfoStealer 恶意代码。该恶意代码会窃取保存在 Chrome、Firefox 和 Internet Explorer 等网络浏览器中的登录信息。

过去，攻击者一直针对的一直是系统信息或是各种程序的登录信息。然而，最近呈现目标正在逐渐扩展到加密货币钱包和游戏等领域。另一方面，目标中排除 Internet Explorer（2018年后，其使用量急剧下降） 的恶意代码数量有所增加。这表明攻击者也在不断发展他们的攻击方式以跟上趋势，从而获取最大的利益。

与其他恶意代码一样，InfoStealer 通过邮件、访问网站和下载程序等方式进行感染。在大部分情况下，攻击者将恶意代码嵌入到 Crack、串行密钥生成程序（Keygen）和密钥管理服务（KMS：Key Management Service）中来分发恶意代码。特别是KMS认证程序，不仅在家庭中广泛使用，在大型企业中也广泛使用，因此恶意代码制作者经常将其用作分发方式。

此外，随着新冠状病毒大流行期间远程办公的推广，将个人计算机或家庭共享计算机用于工作的情况也随之增加。此时，经常会发生在下载破解版以未经许可使用工作所需的程序时感染 InfoStealer 的情况。尽管很少见，但已确认供应链攻击案例。

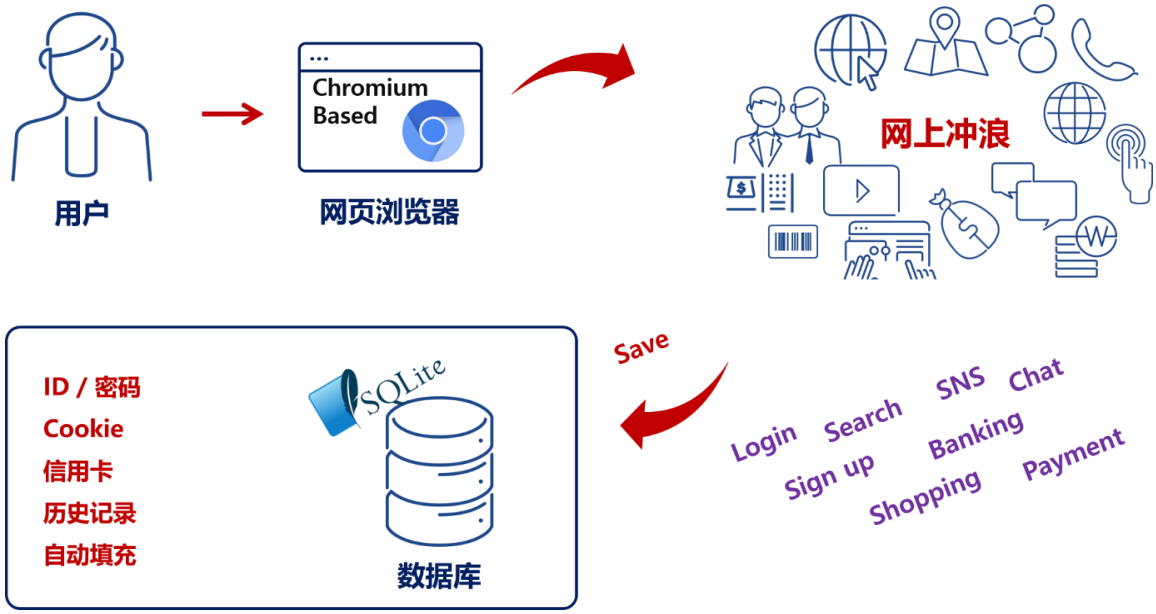
使用“自动登录”功能的信息窃取原理

在本文的开头有提到，如果使用程序和网络浏览器的自动登录功能，使用 InfoStealer 恶意代码来窃取信息变得更加容易。其原因是什么？在相关案例中，让我们来了解一下用户经常遇到的存储于网络浏览器的信息遭到泄露的原理。

1. 基于 Chromium 的浏览器

Chromium 是由谷歌（Google）开发和管理的开源网络浏览器，是目前使用最多的网络浏览器引擎。Chrome、Edge 以及 Opera 等都是基于 Chromium 代码进行开发的代表性浏览器。

基于 Chromium 的网络浏览器在本地系统的 SQLite DB 文件中保存用户在浏览网页时保存的帐户（ID和密码）信息、Cookie 数据、信用卡信息、历史记录、自动填充（Autofill）等。



【图3】浏览器中保存的内容

SQLite DB 文件内部的一些敏感数据由 AES（Advanced Encryption Standard）以加密状态进行管理。Chromium 的加密数据管理仅允许本地系统的用户解密信息，且将 AES 密钥以 DataProtection API 加密的 DPAPI blob 形式保存。该数据由 Base64 编码并保存在（省略）...\User Data\Local State JSON 文件的“os_crypt”：{“encrypted_key”} 位置。

InfoStealer 通过 SQL 查询，从保存帐户、Cookie、信用卡、历史记录和自动填充信息的对象数据库文件中提取必要的数据。然后，通过解密 AES 密钥，收集加密数据的纯文本信息。

项目	路径	表	加密
帐户 (ID/Password)	%LocalAppData%\Google\Chrome\User Data\Default\Login Data	logins	O
Cookies	%LocalAppData%\Google\Chrome\User Data\Default\Network\Cookies	cookies	O
信用卡 (Card)	%LocalAppData%\Google\Chrome\User Data\Default\Web Data	credit_cards	O
历史记录 (History)	%LocalAppData%\Google\Chrome\User Data\Default\History	urls	X
自动填充 (Autofill)	%LocalAppData%\Google\Chrome\User Data\Default\Web Data	autofil	X

【表1】保存在Chromium的主要数据文件

项目	对象文件	SQL Query
帐户 (ID/Password)	Login Data	SELECT origin_url, username_value, password_value FROM logins
Cookies	Network\Cookies	SELECT host_key, name, Path, expires_utc, is_secure, value, encrypted_value FROM cookies
信用卡 (Card)	Web Data	SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
历史记录 (History)	History	SELECT url, title, visit_count, last_visit_time FROM urls
自动填充 (Autofill)	Web Data	SELECT name, value FROM autofill

【表2】Chromium 信息收集 SQL 查询

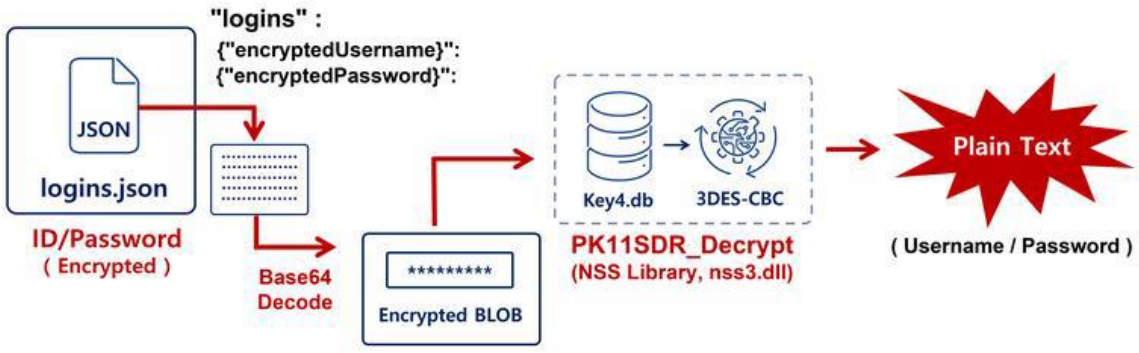
另外，除了密码之外的所有加密字段值都可以使用相同的方法解密成纯文本。可解密的信息包括▲ Cookies 表的 encrypted_value、▲ Credit_Card 表的 card_number_encrypted 字段等。

2.基于 Gecko 的浏览器

Gecko 是由 Mozilla 基金会开发和管理的开源网络浏览器引擎。使用该引擎开发的代表性网络浏览器有 Firefox、Thunderbird、IceDragon 和 Cyberfox。它是仅次于 Chromium 的常用网络浏览器引擎。

保存在 Gecko 浏览器中的帐户信息会以加密状态保存在 logins.json 文件中。Gecko 浏览器的加密数据管理使用 Mozilla 开发的 NSS 库的 PK11SDR_Encrypt / PK11SDR_Decrypt 函数。简单总结一下该函数内部的操作过程，从 key4.db 文件中提取 Master Key 和 Salt 值，并通过 3DES-CBC 运算进行加密/解密。

InfoStealer 动态加载基于 Gecko 的浏览器使用的 nss3.dll 的 PK11SDR_Decrypt 函数，并将从 logins.json 中提取的加密帐户信息解密为纯文本。



【图4】基于 Gecko 的解密过程

基于 Gecko 的浏览器相关主要文件和浏览器信息收集 SQL 查询信息分别如【表3】和【表4】所示。

项目	路径	加密
帐户（ID/Password）	%AppData%Mozilla\Firefox\Profiles\[随机值]\logins.json JSON	O
Cookies	%AppData%Mozilla\Firefox\Profiles\[随机值]\cookies.sqlite	X
历史记录（History）	%AppData%Mozilla\Firefox\Profiles\[随机值]\places.sqlite	X

【表3】基于 Gecko 的主要文件信息

项目	对象文件	SQL Query
Cookies	cookies.sqlite	SELECT host, name, path, value, creationTime, expiry, isSecure FROM moz_cookies
历史记录（History）	places.sqlite	SELECT url, title, visit_count, last_visit_date FROM moz_places

【表4】Gecko 信息收集 SQL 查询

Gecko 浏览器的 Cookie 信息保存在 cookies.sqlite 中，历史记录保存在 places.sqlite 数据库文件中。由于除帐户外都以纯文本形式保存，没有任何加密，攻击者可以轻松获取信息。

针对自动登录的 InfoStealer，其攻击确有发生

如果用户使用网络浏览器或程序的自动登录功能，则个人信息会很容易被 InfoStealer 窃取。而且，在韩国实际已发生了由此类攻击造成的入侵事件，因此需要格外提高警惕。

AhnLab 的 ASEC 分析团队证实，在2021年12月对某企业内部网络入侵事件调查中，用于访问企业网络的 VPN 帐户从一名远程办公的员工的个人计算机中泄露。遭受损失的企业提供了 VPN 服务，以便员工在远程办公时可以访问公司网络，员工在使用公司提供的笔记本电脑或个人计算机连接 VPN 后开始工作。

该员工利用网页浏览器提供的密码管理功能，在网页浏览器中保存和使用 VPN 账号和密码。在这一过程中，感染了针对帐户信息的恶意代码，多个站点的帐户和密码均遭到泄露。其中也包括了该企业的 VPN 帐户，泄露的 VPN 帐户大约在3月后被用来入侵该企业的内部网络。

经确认，该员工的计算机由全家人共同使用，并没有得到安全的管理。致使该计算机长期感染各种恶意代码，即使安装了其他公司的防病毒软件，却没能准确检测到恶意代码并予以修复。

在受感染的恶意代码中，包括了 Redline Stealer 类型的恶意代码。Redline Stealer 程序于2020年3月首次出现在俄罗斯暗网上 ， 收集保存在网页浏览器中的帐户信息。该 Redline Stealer 伪装成音调调节程序——SoundShifter 的破解程序，并在网上传播。用户通过输入软件名称和“破解”、“免费”等关键词来搜索并下载文件，然后直接运行下载文件，从而感染了恶意代码。

最有效的安全方法就是“预防”

如果使用自动登录功能，InfoStealer 会更容易窃取帐户信息，并且相关的受害案例也实际发生。那么，应该怎么做才能尽可能减少此类信息窃取？

当我们感冒时，我们会使用各种方法来治愈和减少痛苦。到医院就诊后，开退烧药或抗生素，或在家喝热茶，好好休息。在大多数情况下，采取这类措施将有助于感冒好转。但从根本上说，最好的办法便是保持健康，不得感冒。为此，我们需要遵循最基本的健康习惯，例如经常洗手，多饮水等等。也基于此，人们在新冠状病毒大流行之后纷纷戴上了口罩。

网络安全，尤其是本文探讨的与信息泄露相关的损害，可以参照上述感冒的例子进行理解。信息泄露后，通过后续措施控制受损程度固然重要，但最好还是遵守基本的安全规则，提前防止信息遭到窃取。首先，在使用网站或程序时最好不要保存帐户信息。当然，这确实是一个方便的功能，但正如我们在本文中所了解到的，保存的信息在感染 InfoStealer 恶意代码时很容易遭到泄露，因此应该尽可能减少使用。

此外，不仅是 AhnLab，其他机构也一直在强调的规则，即“避免”▲下载和使用非法软件、▲访问不受信任的网站、▲运行可疑的电子邮件附件并点击 URL 等。此外，应随时检查防病毒软件等安全软件和正在使用的程序等是否已更新到最新版本。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com
© 2022 AhnLab, Inc. All rights reserved.