密码窃取恶意软件势头正盛

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Still Sexy: Password Stealing Malware		
原文作者	Pat Belcher	**原文发布日期**	2016 年 7 月 14 日
作者简介	Invincea 公司(前身为著名的安全司令部公司)成立于 2006,是一家终端软件安全公司主要专注于企业网络安全防护。 http://motherboard.vice.com/read/the-library-of-congress-was-hacked-because-it-hasnt-joined-the-digital-age?trk_source=recommended		
原文发布单位	Invincea 终端软件安全公司		
原文出处	http://motherboard.vice.com/read/the-library-of-congress-was-hacked-because-it-hasnt-joined-the-digital-age?trk_source=recommended		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

密码窃取恶意软件势头正盛

你的密码价值几何？或许你的银行账户密码值点钱吧，无论里面有没有钱。但和你的社交媒体账户密码相比，和你的免费网络邮箱账户密码相比、和像流媒体娱乐网站 Hulu，Netflix 账户密码相比，恐怕你很难判定哪个更有价值，哪个没有价值。当然了，访问企业内部资源的相关工作密码，也有可能被网络罪犯在地下市场大肆兜售。例如，企业内部网，大事记，工资单，代理服务器，以及虚拟专用网（VPN）等账号密码。

有一个通过武器化 Office 文档发送的恶意软件家族专门窃取存储在本地系统上的密码。但是，和 Invincea 公司追踪的勒索软件（如 Locky，Cerber 和 CryptXXX）活动相比，密码窃取活动更多。但是，如果勒索软件如此轻易得手，有利可图，为什么黑客仍然想要窃取密码呢？恐怕，窃取密码的价值比我们想象的要更大。

过去，人们衡量被盗密码的价值是根据罪犯地下售价而定的。然而，这并不是衡量其价值的唯一标准，可能还不够全面。或许，被盗密码的价值可以根据盗取密码之人决定，而不是二手买家。我们应该怎样确定其价值呢？接下来我们讨论一下窃取密码的机会成本和发动勒索攻击的机会成本，最终看谁的价值更容易量化。

考虑到窃取密码总量与勒索攻击总量持平，这使得网络攻击者每成功感染 4 台主机净赚 750 美元，那就表明，存储在主机上的密码大约值 185 美元。否则，考虑到勒索软件这般普遍和成功，密码窃取攻击者也会干勒索的事了。

发现勒索软件攻击就好比主机一旦被感染，就会显示闪屏一样简单。但是，当密码窃取器把主机上存储的所有密码上传到 C&C 服务器上时，受害人不会发现主机有任何异常。因此，在毫不知情的情况下，你可能成为密码失窃的受害者。

密码窃取恶意软件

为了更深入的了解密码窃取器无处不在，我们将会以 Invincea 公司一位顾客上周遭遇的武器化文档窃取密码事件进行分析。

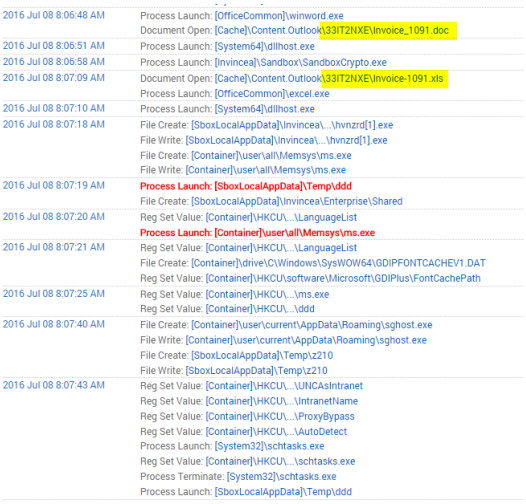


图 1：武器化文档添加了文件名 ddd，并在 Memsys 目录下创建了 ms.exe。

该例中，用户打开了一个 Office 武装化文档，它伪装成来自 Outlook 邮箱的发票。它在该文件 temp 目录下添加了一个无扩展名的 ddd 文件，并且在用户所有 Memsys 目录下依次写入 ms.exe 执行程序。因此，反病毒供应商极难本地识别这种恶意软件。如下，Reversing Labs 画出了一张反病毒引擎识别这种二进制文件的效能图。

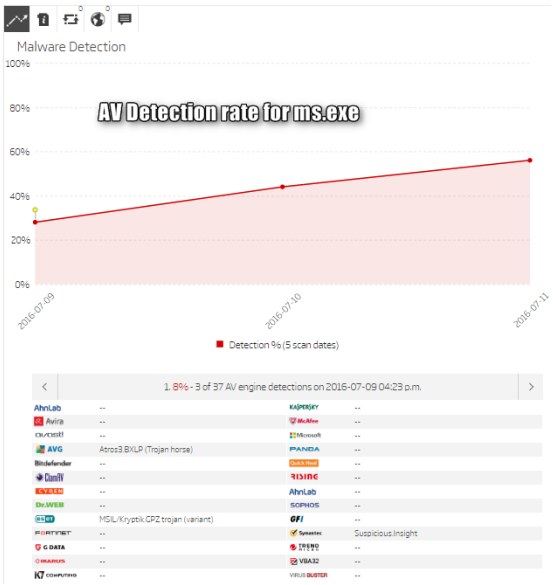
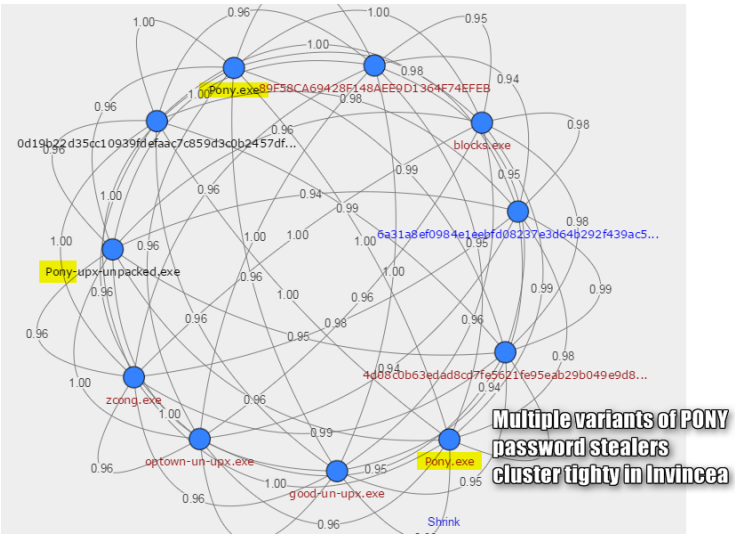


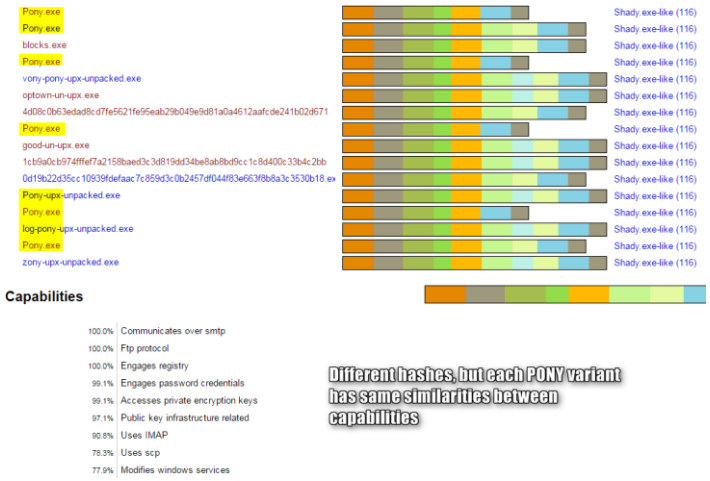
图 2：7 月 8 号，Invincea 阻止了此次攻击，而大多数反病毒公司起初未能识别此类威胁，直到 7 月 10 号。

在 ms.exe 放入 Memsys 目录下之时，Invincea 公司就一直在对类似的感染事件进行追踪。根据美国国防部高级研究计划局赞助的深度学习检测引擎检测，这些二进制文件和 Pony 密码窃取恶意软件家族有关。

这是它们如何在 Invincea 中群集示意图：



另外，每一个二进制密码窃取器都有共同之处，例如，获取 SMTP, SCP, SSH, HTT 密码以及更多的资源。



Invincea 网络风险公司已发现超过 116 个和 Pony 恶意软件家族类似的样本。此外，也有其它具有不同特征的软件家族群聚在一起。但是，这也表明在这 116 起攻击中，罪犯利用 Pony 密码窃取器偷偷的从企业和家庭用户那里盗取密码。原因是他们把武装攻击文档误认为是发票，传票和订单确认信息。这样表示，窃取的密码可能被存储在 116 台不同的服务器上。你可以点击下面的链接浏览二进制密码窃取软件家族信息。

https://cynomix.invincea.com/sample/fba412258cebbe22e8a335d2bbd770556003ca2c

那么，什么类型的密码被盗了呢？通过二进制密码窃取器的字符串信息，我们可以很清楚的看到。

基本上，所有的密码主要存储在本地系统的某个地方例如，注册表，浏览器，本地密码数据库或者关联程序，这些地方黑客都能猜到。然后黑客，把从系统窃取的密码上传到硬编码的 C2 服务器上。

钓大鱼

对攻击者来说，窃取一些僵尸账户密码对他们来说显然毫无价值。但是当数量达到数百个之多，收入就可观了，包括窃取的那些重要基础设施的密码。

当然，对企业来说其中一些被盗密码极具价值。同时，黑客会寻找此类密码助其入侵公司网络，例如基于网络的 VPN，内部资源，代理服务器以及其它的资源。所有的这些资源可以打包，然后通过网络在黑市售卖或者黑客自己使用。

经由 FTP, SSH, HTTP 控制台登录可以获取所有公开互联网资源 Root 访问权限，就其价值来说仅次于窃取密码。因为，Root 访问权限可以给攻击者的其它恶意攻击提供免费的主机进行恶意软件投放和 C2 控制。

SMTP 资源对网络攻击者的重要价值在于它不仅可以提供可用账户发送附件武装攻击垃圾文档，而且劫持账户信息，请求获取邮箱重置，改动密码的权限，例如社交媒体账号。

你应该先改哪一类密码呢？

至今，关于勒索软件泛滥困扰网民的声音一直不绝于耳。现如今，密码窃取恶意软件猖獗程度与勒索软件相比不遑多让。其活动涉及数据之大，以致众多银行和公司大量披露密码存储，并让受害人警惕密码盗窃，这已经成为一种常态。

不要等到第三方告知，你的密码已经被盗了，你才想起去改密码。如果你要改动所有账

号密码，下面的规则会帮助你根据账户的重要性决定改密码的先后顺序。

个人财务：首先保护个人及财务。首先确保银行账户安全。接下来确保所有可以访问网上账户的网站账户安全，包括退休金账户，投资账户，以及税收资源账户的安全。

收入来源：如果怀疑你的工作账户已失窃，你应首先保护你的收入来源账户的安全，再去挽救这些有用的东西，包括公司使用的所有云服务和的媒体账户。

邮箱账户: 由于很多服务经邮箱通知发出警报或者提供改动密码的访问路径，因此接下来你要确保邮箱访问路径安全。

电话账户：如果攻击者知道了你的线上服务密码，例如 ITunes 账户，那么你的智能手机很可能被入侵了。

订阅账户: 然后接下来应该确保设置的自动转账服务账户安全，包括流媒体娱乐账户，学校午餐项目账户，草坪修理费账户等。

社交媒体：除非你是名人或者是名牌，社交媒体账户几乎可以忽略不计，所以把它们放到最后修改密码。

除上述之外的其它账户：如果你不确定还有其它的要修改，检查你保存在 URLs 网页浏览器上的密码。从浏览器帮助菜单上你可以知道如何获取保存的密码。然而，很多人喜欢所有的账户都使用一次性的，例如从网上照片存储到外卖 pizza，所以像这些都需要改动密码以防非法访问。

为提高安全性 账户应尽可能多的使用双重验证。如果将来密码因为双重验证服务被盗，那么它将因为无法访问身份验证机制而变得毫无价值。

结论

不久之前，CPU 周期和密码猜测程序曾被用来破译密码。迫于这种威胁，增加密码的复杂度，长度，通行口令，以及密码的独特性成为安全的关键所在。但是如果武装攻击文档可以在你不知道的情况下轻易获取你网上所有资源账户设置的超复杂、特别的密码，那么之前所做的一切都白费了。

密码窃取活动所获数据之大媲美勒索活动最盛之时。确保账户安全的最好方式是使其毫无利用价值。这就使得双重验证随时随地可行。在改其它账户密码的时候，不要经常使用双

重验证，但至少要超过账户密码量的 1/4。