调查报告

了解密码窃取活动的内幕：到底是谁窃取了身份信息以及他们是如何窃取的

作者：Dennis Elser 与 Micha Pekrul，McAfee® Avert® Labs

目录

随着如今网上购物和银行交易的日益频繁，密码窃取已成为一种常见的网络犯罪行为。无论采用何种攻击媒介，在许多情况下，一些密码窃取恶意软件总是能够设法侵入受害者的计算机。

传播恶意软件的犯罪组织通常在俄罗斯、中国或巴西等国家/地区从事非法活动；他们唯一的目的就是获取用户凭据并使其转换为现金。在经济不稳定时期，窃取的凭据比以往任何时候都更具价值，因此请务必保护好您的隐私和身份信息。

此报告介绍了当前最先进且流行的密码窃取恶意软件系列所采用的攻击技术，以及用于攻击银行最新安全机制的伎俩（如屏幕键盘），还剖析了密码窃取行为的新目标 - 大型多人在线角色扮演游戏 (Massive Multiplayer Online Role-Playing Game, MMORPG)。

流行程度和传播途径

McAfee Avert Labs 发现，2007 至 2008 年间，密码窃取恶意软件变种的数量增加了近 400%。

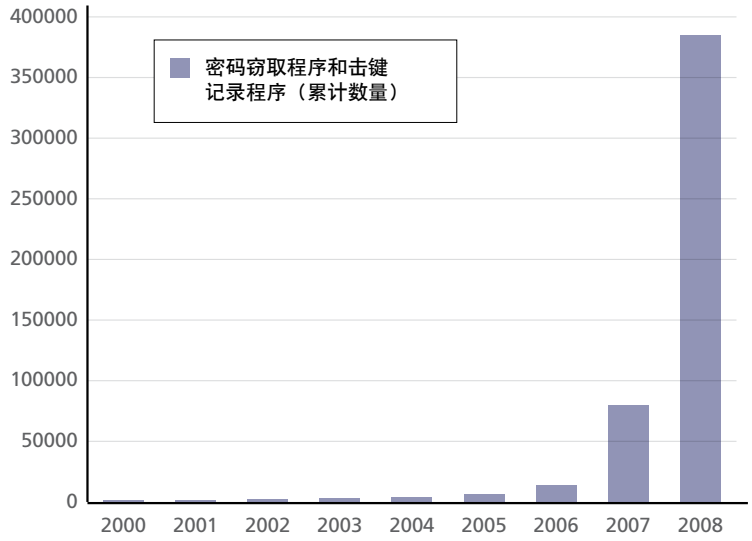

图 1：密码窃取恶意软件的增长。（除非另外注明，所有图形均来源于 McAfee Avert Labs。）

尽管在过去密码窃取程序感染游戏的现象并不常见，但是在 2006 年和 2007 年此类感染也呈现增长趋势。[1] 在此期间，涉及虚拟游戏商品（如刀剑、头盔和技能点数）交易的地下经济迅速发展。这些虚拟商品在出售给希望提高游戏技能和得分、又不愿意在游戏上耗时太多的其他玩家后，即可转换为真金白银。“打金” (gold farming) 在一些国家/地区已经成为一种谋生方式，例如，在中国就有成千上万的打金者在努力收获尽可能多的虚拟价值，然后出售给全球范围内更为富有的玩家。

1. Dr. Igor Muttik, “Securing Virtual Worlds Against Real Attacks–The challenges of online game development” (Igor Muttik 博士，“保护虚拟世界免受现实世界的攻击 - 在线游戏发展所面临的挑战”)，McAfee Avert Labs。www.mcafee.com/us/local_content/white_papers/threat_center/wp_online_gaming.pdf

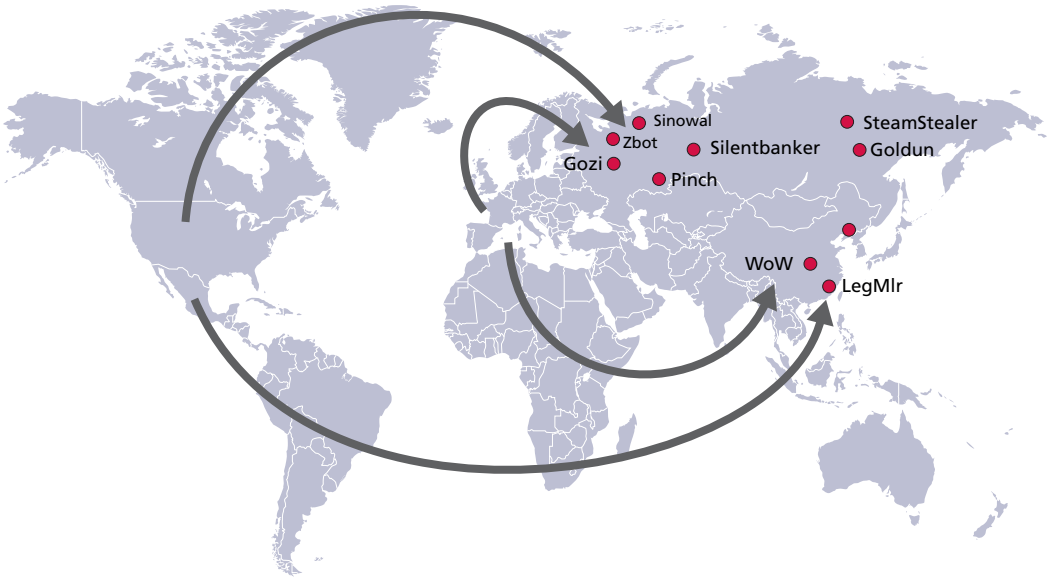

图 2：每个恶意软件系列所窃取身份信息的当前传回原址目的地国家/地区。

用户面临各种形式的数据窃取威胁，恶意软件并不是唯一的数据窃取形式。例如，网络钓鱼也是一种虚拟窃取形式。其目的与恶意软件相同，即窃取受害者的凭据，但它并不使用恶意代码。该攻击完全依赖于社会工程技术，让缺乏防范意识的用户泄露自己的密码。进行网络钓鱼攻击的虚假网站可能会达到以假乱真的效果。

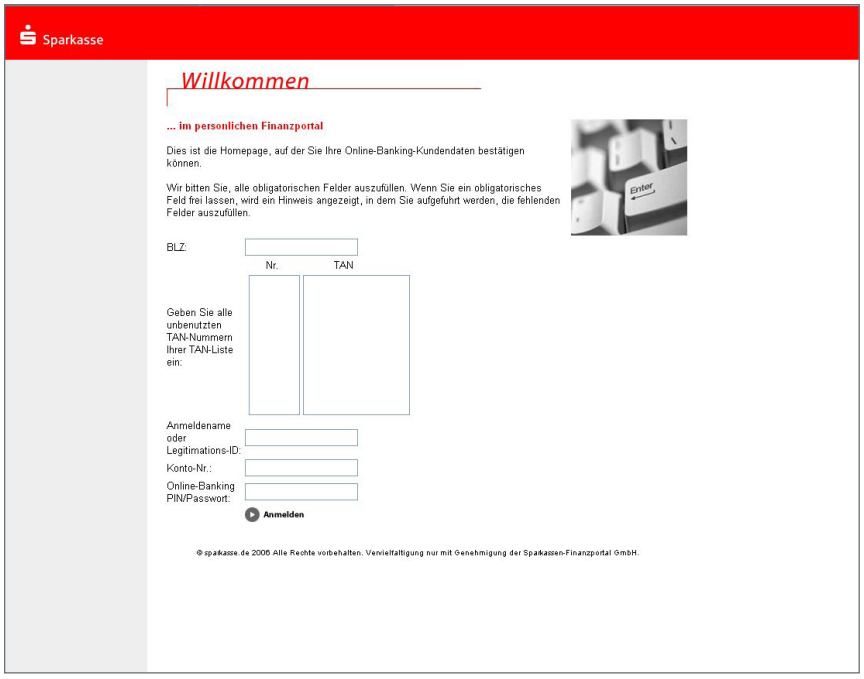

图 3：该网络钓鱼站点索要所有未使用的交易身份验证号码 (Transaction Authentication Number, TAN) 以及索引编号，以便攻击者可以攻破高级 iTAN 系统

垃圾邮件是密码窃取程序的主要传播途径之一。通过发送大量邮件（如虚假发票或虚假不间断电源系统 (Uninterruptible Power System, UPS) 通知）诱使用户打开看似合法的 PDF 附件，并最终使用户运行侵入其系统的可执行文件。垃圾邮件的主题常常根据目标读者量身定制，并充分利用目标国家/地区当地的潮流趋势、政治新闻或热门话题。

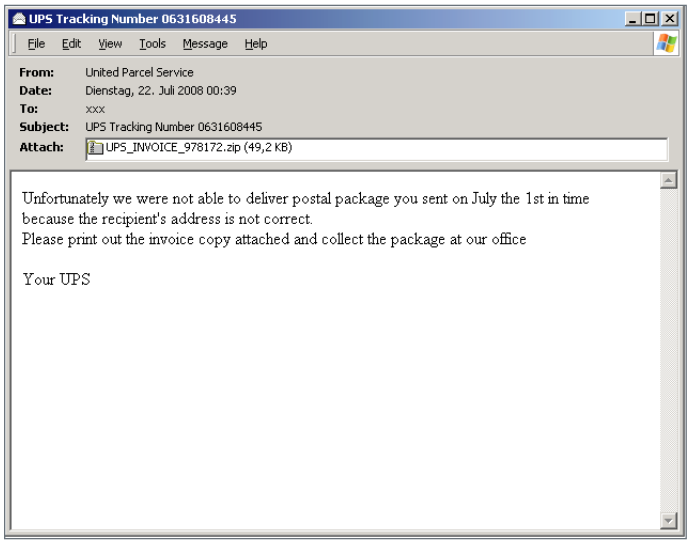

图 4：传播 Zbot 恶意软件的典型垃圾邮件。

除了网络钓鱼、垃圾邮件和其他常见的社会工程手段之外，另一种日益流行并且能有效感染用户 PC 的方式是基于浏览器的攻击。[2] 通过使用所谓的“病毒感染因素”(drive-by infection)，攻击者可以自动侵入数千个网站，从而使用合法及受信任的网站来传播恶意代码。黑客甚至借助搜索引擎来寻找潜在的易受攻击网站。他们通常在这些网站中注入脚本或 IFrame 元素，以将受害者指向恶意代码（来自攻击者主服务器或直接托管在受感染的站点上的恶意代码）。访问这些受感染网站的用户最终会在毫不知情的情况下请求并执行恶意代码。

猫鼠游戏：银行系统不断发展，攻击者步步紧逼

密码窃取恶意软件的演化与数字安全设备和措施的发展紧密相关。对于仅依赖用户名与密码组合的简单身份验证因素，使用简单的击键记录程序即可轻松破解。只要对安全机制加以改进（例如，引进“外部”身份验证因素），击键记录程序便无法得逞。“易记字词”(memorable word) 即可作为这样的附加因素。网上银行系统要求用户仅提供预定义的部分字词，这样，即使击键记录特洛伊木马程序使出浑身解数，也无法捕捉到所有信息。如今，攻击者面对的是受多因素身份验证系统保护的系统。在欧洲广泛应用的典型多因素身份验证使用的是交易身份验证号码（或 TAN）。这些号码是指银行提供的大量一次性密码，对于每笔交易，用户都需要选择一个 TAN 来完成身份验证。提高安全性的下一个步骤是编制索引的 TAN (iTAN)，即，将 TAN 与索引编号结合使用。网上银行系统会为每笔交易指定一个随机选择的索引（属于特定 TAN）。

图 5：Blizzard 的一次性密码令牌。（来源：Blizzard Entertainment）

其他多因素身份验证系统或强大的身份验证系统属于加密设备，用于创建仅在短时间内有效的一次性密码。这些安全令牌通常用于公司网络中。但即使像热门在线游戏**魔兽世界**的开发商 Blizzard 这样的公司，也引进了安全令牌技术用于身份验证。[3] 现代安全系统都具有硬件 TAN 生成器，生成器还需要用户提供银行卡并成功完成质询-响应过程。

2. Christoph Alme，“Web 浏览器：新的威胁攻击对象”，McAfee Avert Labs。www.mcafee.com/us/local_content/white_papers/wp_webw_browsers_w_zh_cn.pdf
3. www.blizzard.com/store/details.xml?id=1100000182。

每当出现一种新的防护技术，密码窃取程序也会随之作出相应的调整。例如，当银行引入了要求用户点击相应数字而非键入数字的虚拟键盘技术后，恶意软件作者立即作出响应，实施了屏幕捕捉技术。另一种常见技术是 Web 注入，恶意软件将附加的表单字段添加到银行的网页中，并要求用户提供其他详细信息，如 ATM PIN 码、完整的“易记字词”或用户的身份证号码。由于这些注入的元素看似合法且不易引起怀疑，因此用户很难发现它们。

恶意软件作者不仅对最新技术步步紧逼，甚至还试图先发制人，这已经不是什么新闻了。为了避免必须将密码获取表格设计为与目标银行网站的安全防范措施和布局相匹配，攻击者会将 DNS 服务器或主机文件重定向到自己的服务器。试图连接到美国银行 (Bank of America) 网站的受感染用户将被定向到一个由其他服务器托管的相似网站上，此服务器当然属于攻击者。使用 DNS 劫持的另一种情况是通过窃听网络通信在远程充当“中间人”(man in the middle)，然后将（修改的）通信重新路由到真实的目的地，反之亦然。

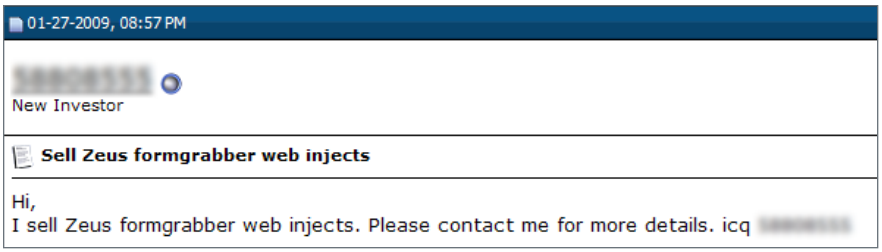

图 6：地下恶意软件市场上出售针对目标网站的自定义布局而设计的“Web 注入”。

在本地实施的劫持攻击并不需要依赖诸如 DNS 之类的特定协议。每当使用了不可预知的 TAN 时，潜伏在受感染系统上的恶意软件即会等待并检测用户输入的凭据。由于这些是一次性的密码，恶意软件首先会保存 TAN，而不让其到达目标银行，然后向用户显示一条虚假错误消息，报告 TAN“错误”。通过拦截已建立的连接，然后使用垃圾代码覆盖身份验证号码，即可以被动形式完成以上任务。或者，可以通过向用户显示一个自定义的虚假弹出窗口，主动完成此任务。

稍后我们会详细讨论此类密码窃取特洛伊木马程序。

Sinowal 和 StealthMBR：当今最令人厌恶的密码窃取程序和最隐蔽的 Rootkit

Sinowal 是一个广泛传播的密码窃取特洛伊木马程序，此木马程序与 StealthMBR（也称为 Mebroot）一同侵入计算机，后者为当今最复杂且最隐蔽的 rootkit 之一。StealthMBR rootkit 会感染硬盘的主启动记录，以便在操作系统启动前控制系统，并且深入到 Microsoft Windows 内部结构中。每次重新启动系统时，rootkit 都会下载其他的密码窃取组件，并且不会将这些组件保存在硬盘上，而是直接让特洛伊木马程序使用 SetWindowsHookEx() Windows 应用程序接口 (API) 函数将自身注入正在运行的进程中。

除了 rootkit 的隐秘性外，新下载的特洛伊木马程序还将使用其他隐蔽机制。早期的 Sinowal 变种除了使用 XOR 加密的字符串外（例如，主机名），还会检测沙盒环境，并且当怀疑自己被观察时，就会隐蔽其行为。但是，在真实的计算机系统上，会跳过某些 Windows API 函数，而转到属于特洛伊木马程序代码的自定义函数。犯罪分子的意图即是让特洛伊木马程序窃取这些函数处理的敏感数据。特洛伊木马程序实施的 API 挂钩技术，会将跳转指令添加到先前合法的操作系统代码中（如图 7 所示），从而在执行合法代码前将控制流转到恶意代码。

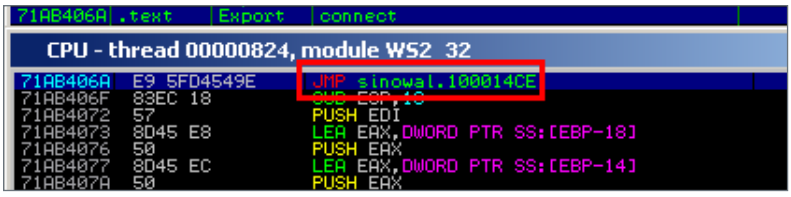

图 7：从 ws2_32 库的 connect() API 跳转到 Sinowal 的代码。

通过检查内存中库的代码是否有任何跳转及其跳转的目的地，安全软件可检测（和删除）这些类型的 API 挂钩。Sinowal 也使用此技术来绕过安全软件（如，个人防火墙或主机入侵防护系统 (Host Intrusion Prevention System, HIPS)）设置的 API 挂钩，以达到自身的目的。一旦 Sinowal 检测到挂钩的 API 函数，将会尝试解码跳转和调用指令以找到 API 的“真实”地址，这样就不会调用安全产品的代码，用户也不会收到有关可疑恶意软件行为的通知。

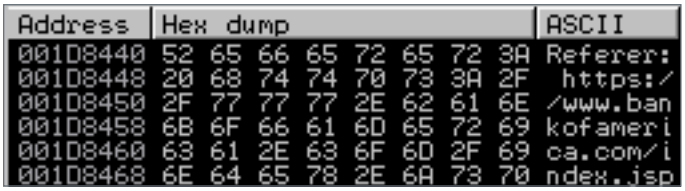

图 8：浏览器将按照在 HttpSendRequestA() API 中显示的样式来设置引用网站。

被跳转的函数是在 Internet 上通信的应用程序广泛使用的函数，这点并不奇怪。当特洛伊木马程序活动时，将会监视 Web 浏览器、电子邮件和 FTP 客户端以及任何其他使用 ws2_32.dll、wininet.dll、nspr4.dll (Firefox)、crypt32.dll 和 advapi32.dll 导出的函数的应用程序，这些函数用于处理敏感信息。如果 Sinowal 在 Internet Explorer 环境中运行，则可能将 HttpSendRequestA()API 用作挂钩函数。在允许代码执行流到达其目的地（原始 wininet::HttpSendRequestA）之前，将首先执行跳转操作。然后解析该函数的 lpszHeaders 参数以获取引用网站，用户浏览网页过程中每次点击超链接时浏览器都会设置引用网站。（HTTP“引用网站”标头中含有前一网站的 URL，该网站**引用**到当前请求的新资源。）根据特定的引用网站，Sinowal 将使 Internet Explorer 显示一个上下文相关弹出窗口，窗口的标题设置为“高级信用卡验证”，要求用户输入详细的信用卡信息。恶意的弹出窗口通过 Internet Explorer COM 接口注入。

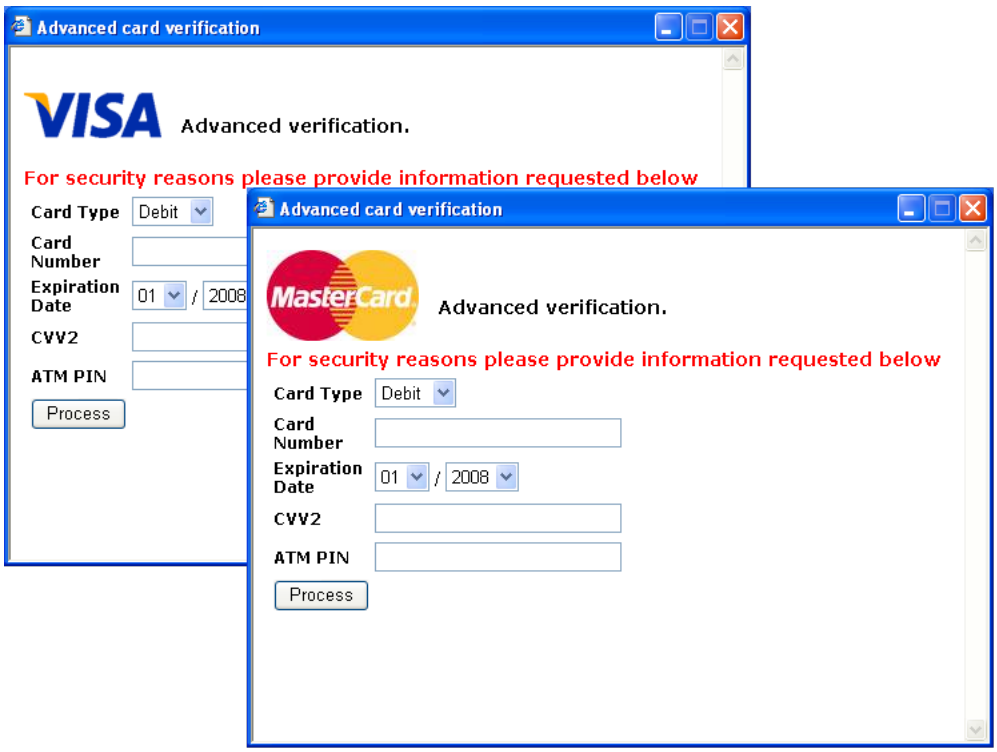

图 9：Sinowal 特洛伊木马程序注入的弹出窗口旨在捕获用户的凭据。

如图 9 所示，用户将看见一个虚假的 VISA 或 MasterCard 弹出窗口，具体取决于其在电子商务站点选择的付款方式。用户甚至不能“无意中”隐藏弹出窗口，因为 Sinowal 使用了 SetForegroundWindow() 函数将弹出窗口置于其他窗口之上，并以无限循环模式执行此操作。然后，会在将特洛伊木马程序窃取的信息发送到犯罪组织（以前称为“俄罗斯商业网络”，其 IP 地址被硬编码到木马程序的代码中）之前对其进行加密。您可能认为将所有加密技术纳入 HTTPS 和 SSH 协议中便可安全无忧，然而恶意软件可分别在加密**前**或解密后获取任何数据。

Sinowal 的最新变种

最新几代 Sinowal 病毒在策略和代码方面都发生了重大变化：该系列从全局范围内收集的数据有所减少（例如，在操作系统级别挂接较少的 API 函数），然而却通过直接锁定特定应用程序在窃取数据方面取得了更大的成功。与先前的几代 Sinowal 特洛伊木马程序相比，该系列使攻击者在以下几个方面获益：

- 减少了数据和通信开销
- 不会通过内存中的 API 挂钩轻易发现特洛伊木马程序
- Sinowal 的兼容性更好。前几代 Sinowal 病毒都是与特定的 Internet Explorer 版本绑定，较新的几代病毒具有更高的独立性，可在各种浏览器版本中通用

最新几代 Sinowal 病毒在从 Windows 注册表中获得凭据的准确位置后即可直接在磁盘上查找凭据。通过在磁盘上“修补”本地安全软件（特洛伊木马程序的天敌）可直接将其锁定和禁用。攻击者的域名不仅进行了硬编码，而且还使用一种基于当前日期的算法进行了计算。前几代特洛伊木马程序拥有大规模数据窃取功能，可在数据挖掘准备阶段用于收集恶意情报，然后下几代特洛伊木马程序会借助这些情报生成最佳结果。

通过使用 FindFirst-/FindNextUrlCacheEntry() API 函数查找 Internet Explorer 自动保存的登录帐户和密码组合；通过读取和解析“signons.txt”、“signons2.txt”和“signons3.txt”文件（保存所有用户私人信息的文件）检索 Firefox 浏览器自动保存的凭据。相当多的应用程序都受到了类似的攻击：Microsoft Outlook、Eudora、Mozilla Thunderbird、VanDyke SecureCRT、WinSCP 和 PuTTY，这只是其中一小部分。与早期的挂钩函数相比，新的攻击方法采取了更不易引起怀疑的技术窃取用户在对话框中键入的密码、个人识别号码 (PIN) 和 TAN：一个后台线程在桌面窗口中循环，查找特定的窗口标题和类，这些标题和类可能指示正在使用一般的密码对话框或特洛伊木马程序明确支持的某些财务应用程序的对话框。然后，将通过向对话框发送一条 WM_GETTEXT 窗口信息来获取密码、TAN 或 PIN。这对于设置了密码字符（星号）的情况同样有效，因为特洛伊木马程序将在读取密码前禁用此类视觉混淆功能，然后再使用 WM_SETPASSWORDCHAR 重新启用此功能。此操作可在瞬间完成，用户并不会注意到有任何异样。

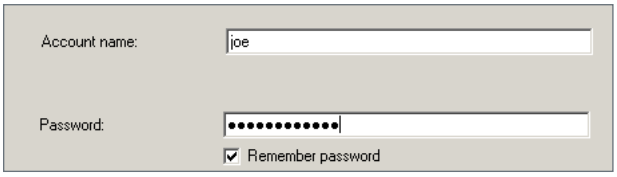

图 10：传统密码对话框。

不仅受感染系统的安全和隐私遭受了感染本身的侵害，站点的可信度在某些方面也受到损害。旨在加强安全的软件（如浏览器插件，也称为浏览器辅助对象）可发出指示安全连接到银行网站的可视信号，如通信灯图标。恶意软件只需在磁盘中为这些插件安装修补程序即可更改其行为，这样插件可能会显示已建立安全连接，但事实上并没有建立任何安全连接。由于恶意软件要查找特定字节类型的代码以安装修补程序，因此，恶意软件作者拥有了对安全产品进行反向工程的另一个理由。通过滥用用于安全通信的第三方商业库，即使是加密或哈希化密码也可通过暴力攻击破解。当前 Sinowal 变种的一个更加危险的“功能”是可以将受感染用户

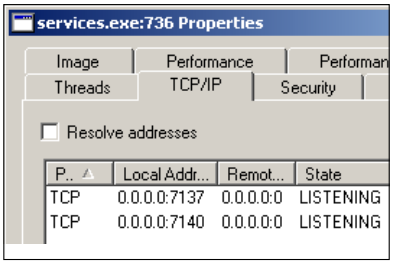

图 11：在具有系统权限的进程中运行的代理服务器。

的计算机变成一个面向全球开放的代理。达到此目的的方法是，将其代理服务器代码注入到 services.exe 进程，该进程是一个使用系统权限运行的应用程序。注入代码后，受感染的进程会连续接受任何入站 HTTP-、SOCKS4- 和 SOCKS5- 代理连接。因此，攻击者可以发动第二阶段攻击，滥用受感染主机的地理位置和声誉。

任何一个感染都会让您的免疫系统瘫痪

似乎受害人的身份被**一个**恶意软件单独感染和劫持还不够，恶意软件的 HTTP 代理代码又在受感染的计算机上打开了另一个缺口。因为攻击者并不在意写入安全代码，Sinowal 代理中的错误（如同其他主要恶意软件系列一样）会将计算机开放，以通过执行远程代码发动进一步攻击。

```
copy_buffer_to_stack:
inc     esi
mov     cl, [esi]
mov     [eax], cl
inc     eax
dec     [ebp+len]
mov     [eax], bl
cmp     [esi], dl
jnz     short copy_buffer_to_stack
```

图 12：错误的 HTTP 代理代码。

单个恶意软件感染可通过以下攻击媒介造成无数的下游感染：

- 攻击者命令受感染的 PC 下载其他恶意软件组件
- 攻击者是 bot 操纵者，他将受感染的 PC 租给其他攻击者，后者会在受害人的 PC 上下载并执行其他恶意软件
- 其他攻击方会搜索被特定恶意软件感染的系统，然后远程利用此恶意软件的“漏洞”

之前已经提到，恶意软件作者会对安全软件进行反向工程，那么他们为什么不对其竞争对手的恶意软件进行反向工程，从而获得更大的“市场份额”呢？最近一个以非传统方式删除竞争对手恶意软件的示例是 Tigger rootkit，[4] 它利用 Windows 代码中的本地漏洞 (MS08-066) 为恶意软件授予系统权限，从而禁用安全产品并删除竞争的恶意软件。

如图 12 所示，Sinowal HTTP 代理代码中的一个漏洞由一个循环构成：通过 Internet 将用户提供的缓冲区中的数据复制到一个有限的堆栈缓冲区，直到在用户提供的缓冲区中发现某一特定字符。输入格式错误的内容会造成对各个缓冲区的写入超出自身限制，从而使其他攻击者可以在受感染的受害者计算机上更随意地执行恶意代码。这使得其他潜在攻击者可通过覆盖关键数据（例如，结构化异常处理 (Structured Exception Handler, SEH)、堆结构和堆栈中的函数返回地址）获取控制权。尽管 Windows 提供了内置的安全机制以防止在保存数据的内存区域中执行代码，以及阻止成功覆盖 SEH[5]，但是这些机制可被设定为无效，因为任何应用程序都可以自行决定这些措施是否在特定的应用程序进程中生效。

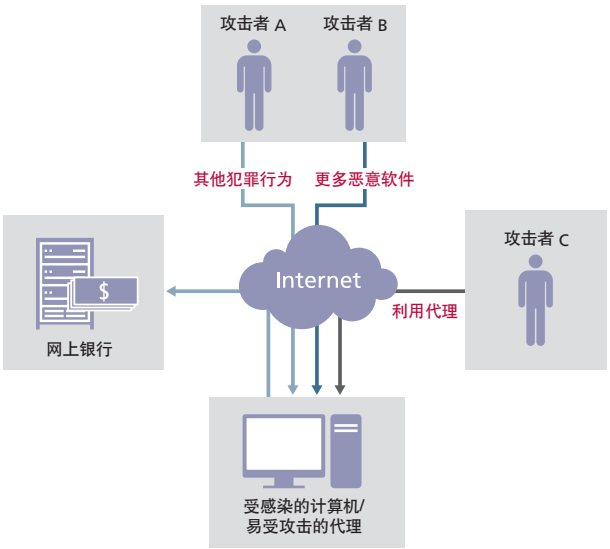

图 13：不同的攻击情况

4. http://mnin.blogspot.com/2009/02/why-i-enjoyed-tiggersyzor.html。
5. http://blogs.technet.com/swi/archive/2009/02/02/preventing-the-exploitation-of-seh-overwrites-with-sehop.aspx。

我们不会期待恶意软件作者会使用 /GS 或 /NXCOMPAT（引导编译器生成更安全代码的标记）编译他们的产品，这一点不足为奇。

如果 Sinowal 中存在堆栈缓冲区溢出的情况，则可以远程覆盖所有“剩余”字段（位于缓冲区后面）以及最为重要的、负责任意代码执行的指针。当前已知的主要威胁的有效期“仅”有几个星期，因为通过安全公司和执法部门的合作，恶意软件的命令和控制服务器能够很快得到控制。一旦受到控制，密码窃取恶意软件便无法将其窃取的凭据传回原址；但是在高权限进程环境中运行的漏洞代理服务器将使受感染的计算机受到进一步的攻击。自 2006 年以来，此代理代码的存在及其可能的漏洞已经为地下社区所熟知。

Zbot：下一代击键记录程序

Zbot 是另一个针对金融行业的数据窃取恶意软件系列，其主要窃取对象为银行 PIN 和 TAN。与前几代 Sinowal 相比，Zbot 特洛伊木马程序同样挂接许多用户模式的 API 函数，从而实时获取凭据。不同之处在于，Zbot 通过用户模式的 API 挂钩来获得凭据，而不是使用 Sinowal 附带的 rootkit 组件包含的内核模式挂钩。针对 ntdll.dll 的 NtQueryDirectoryFile() 函数（由 FindFirst-/FindNextFile() API 函数调用的本机 API）的跳转，可以筛选用户看不到的一些目录名和文件。

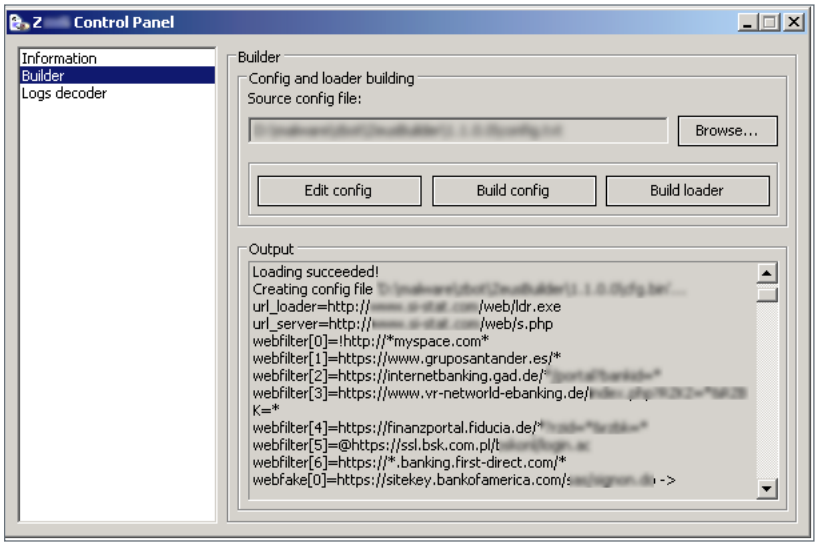

图 14：只需单击鼠标，Zbot 构建工具包就能够生成新的变种。

此外，还设置了另外几个本机 API 函数（如 NtCreateThread()、LdrLoadDll() 和 LdrGetProcedureAddress()）的挂钩，以便将恶意代码注入到新创建的进程和线程中，并确保其自身的 API 挂钩持续有效。与 Sinowal 一样，Zbot 特洛伊木马程序通过挂接属于网络 API 的代码实时窃取凭据。这些挂钩通过拦截客户端上的通信（在其到达网络之前）来实施本地中间人攻击。可以将特洛伊木马程序配置为只针对特定主机（如大银行的网站）上的会话，也可以将其用于窃取全局范围内的凭据和主机名。例如，InternetReadFile() 挂钩将查找典型的 HTML 标记；相反，跳转的 send() 函数（位于 ws2_32.dll 中）将检查缓冲区，以寻找任何看似 FTP 协议的内容。“User”、“pass”、“feat”、“pasv”、“list”、“nbsp;”、“br”或“script”等谓词和关键字可能会触发特洛伊木马程序的记录或修改功能。

图 15：Zbot 恶意软件系列当前活跃的命令和控制服务器。（来源：abuse.ch）

为 TranslateMessage() 安装的跳转是 Zbot 最具欺诈性的跳转之一；TranslateMessage() 是一个 Windows 函数，能够将虚拟键盘代码转换成可读取的字符。特洛伊木马程序正是在此将自身插入进来，并通过拦截 WM_KEYDOWN 消息和记录任何字符（例如，凭据）来充当传统的击键记录程序。然而，真正隐秘的部分是拦截 WM_LBUTTONDOWN 窗口消息的跳转，这些 WM_LBUTTONDOWN 窗口消息是指示单击了鼠标左键的事件。对于每次单击（最高限额为 20 次），将以鼠标光标为中心创建正方形的屏幕快照，用于以图形方式捕获用户使用虚拟键盘或屏幕键盘提供的凭据。网络犯罪分子对于此类“图形化击键记录程序”具有超常的敏感度。这是一种典型的猫鼠游戏：在网上银行机构决定从基于键盘的传统验证方式过渡到基于虚拟键盘的专有认证机制后，攻击者立即采取了应对措施。

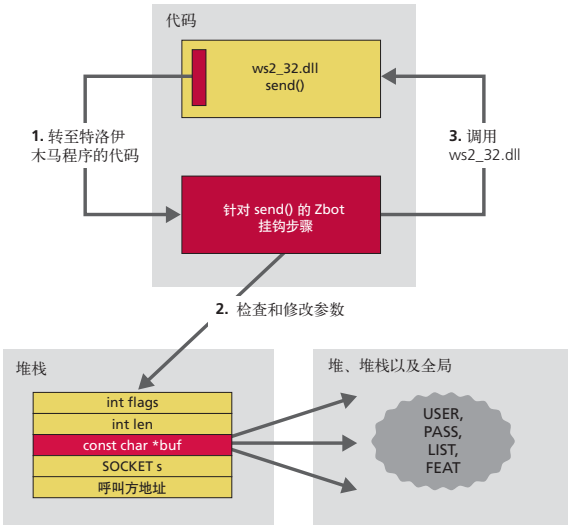

图 16：以图形方式说明 Zbot 的 send() API 挂钩。

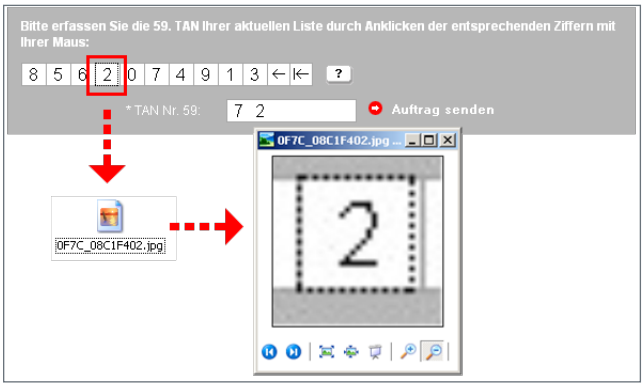

图 17: 下一代击键记录程序从虚拟键盘窃取数据。

屏幕快照将以 JPEG 文件的形式存储到“screens”子目录下，该目录通过特洛伊木马程序的 rootkit 功能隐藏起来，用户永远不会无意中发现这些文件。所有文件名都由多个部分组成，例如，与当前正在运行的进程相关的身份信息、一个下划线字符以及当前时钟计数。借助此信息，便可按时间顺序将点击的密码轻松组合成完整的 TAN。

Sinowal 和 Zbot 共有的另一个“功能”是 SOCKS 代理，Zbot 在该代理中有一个内置后门程序，用于侦听随机选择的传输控制协议 (Transmission Control Protocol, TCP) 端口。在此后门程序支持的一组命令中，有一个使用专有协议来创建和发送屏幕快照的函数。攻击者可能根据受害者的带宽提供足够的编码（例如，GIF、JPEG 或者 BMP）。但是，通过发布能够删除注册表根项“HKEY_CURRENT_USER\Software”、“HKEY_LOCAL_MACHINE\Software”和“HKEY_LOCAL_MACHINE\System”下所有子项的后门程序命令，可导致更严重的后果 - 受感染的系统将完全无法使用。攻击者在滥用被侵入主机的 IP 地址作为攻击源发动攻击后，可以远程破坏被侵入系统以消除他们的踪迹。

Steam Stealer 和地下游戏凭据交易市场

Steam Stealer 是另一种密码窃取程序，与 Sinowal 和 Zbot 这两个专业密码窃取程序相比，Steam Stealer 比较少见。其代码具有模块化结构，这表明该程序中可能存在构建工具包或从其他恶意软件窃取的各种代码段。存在各种代码段的解释似乎更为合理，因为恶意软件可以通过嵌入到可执行文件中的资源进行配置，因此无需使用单独的构建工具包。该代码存在多种缺陷，如大量使用失效的库函数，值得庆幸的是，这些缺陷没有使恶意软件更加强大。Steam Stealer 利用第三方商业工具来破解其获取的凭据。总而言之，该程序仿佛是由可在非法论坛上找到的代码段和第三方二进制文件拼凑出来的产物。

Steam Stealer 在试图窃取游戏玩家的财富之前，会使用几种众所周知的方法来检测虚拟机。简单的方法是调用 GetCurrentUser() API 函数，并参照已知被纳入某些沙盒的用户名单来检查其结果。其他一些方法旨在通过探测某种硬件寄存器的值来检测虚拟操作系统。由 x86 汇编代码序列形成的字节模式极其特别，因此，许多防恶意软件产品都可轻松将其检测和标识出来。为了弥补此缺陷，恶意软件作者决定在恶意软件跳转到此字节模式之前，通过在堆栈上动态构建其代码（由少数几个字节构成）来隐藏此字节模式。Windows XP SP2 中引入的 Microsoft 数据执行预防 (Data Execution Prevention, DEP) 可以检测到试图在堆栈上执行的代码。为所有进程启用 DEP（对于某些 Windows 平台，这并非默认设置）之后，恶意软件将会崩溃并无法造成进一步的危害。Steam Stealer 还会使用其他一些检测方法（如探测是否存在某些安全产品），这些方法就像尝试打开 Windows 注册表中某些项或按名称将进程和加载的库列入黑名单等操作一样简单。

	A
1	Counter-Strike (Retail)
2	The Gladiators
3	Gunman Chronicles
4	Half-Life
5	Industry Giant 2
6	Legends of Might and Magic
7	Soldiers Of Anarchy
8	Unreal Tournament 2003
9	Unreal Tournament 2004
10	IGI 2: Covert Strike
11	Freedom Force
12	Call of Duty 2
13	Call of Duty 4
14	Microsoft Windows Product ID and CD Key
15	Battlefield 1942
16	Battlefield Vietnam
17	Need for Speed Most Wanted
18	Black and White
19	Empire Earth II
20	Medal of Honor Airborne
21	Battlefield 1942 (Road To Rome)
22	Battlefield 1942 (Secret Weapons of WWII)
23	Command & Conquer 3 Tiberium Wars
24	Command and Conquer 3 Kanes Wrath
25	Command & Conquer Generals (Zero Hour)
26	Crysis
27	James Bond 007: Nightfire
28	Command & Conquer Generals
29	Global Operations
30	Shogun: Total War: Warlord Edition
31	Medal of Honor: Allied Assault
32	Medal of Honor: Allied Assault: Breakthrough
33	Medal of Honor: Allied Assault: Spearhead
34	Need For Speed Hot Pursuit 2

图 18：Steam Stealer 攻击的游戏列表。

然而，Steam Stealer 却有一定的商业市场：恶意软件作者以每个 60 欧元的价格出售自定义恶意软件，并且可以根据客户的需求进行度身定制。与恶意软件捆绑出售的还有一个售价为 40 欧元的可执行文件包装程序，该包装程序的作用是使恶意软件“FUD”（网络犯罪领域的一个术语，表示可执行文件“完全检测不到”）。这些可执行文件包装程序或加密程序通常被称为联编程序，因为它们像传统安装程序一样运行。它们丢弃并执行捆绑和加密的二进制文件（可以选择仅针对内存），因此按访问扫描程序不会发现和扫描丢弃的文件。借助公开提供的 VirusTotal.com 之类的服务，或通过“脱机”命令行扫描，网络犯罪分子可以使用联编程序来扫描和修改其新生成的变种程序，直到这些变种无法被检测到为止。

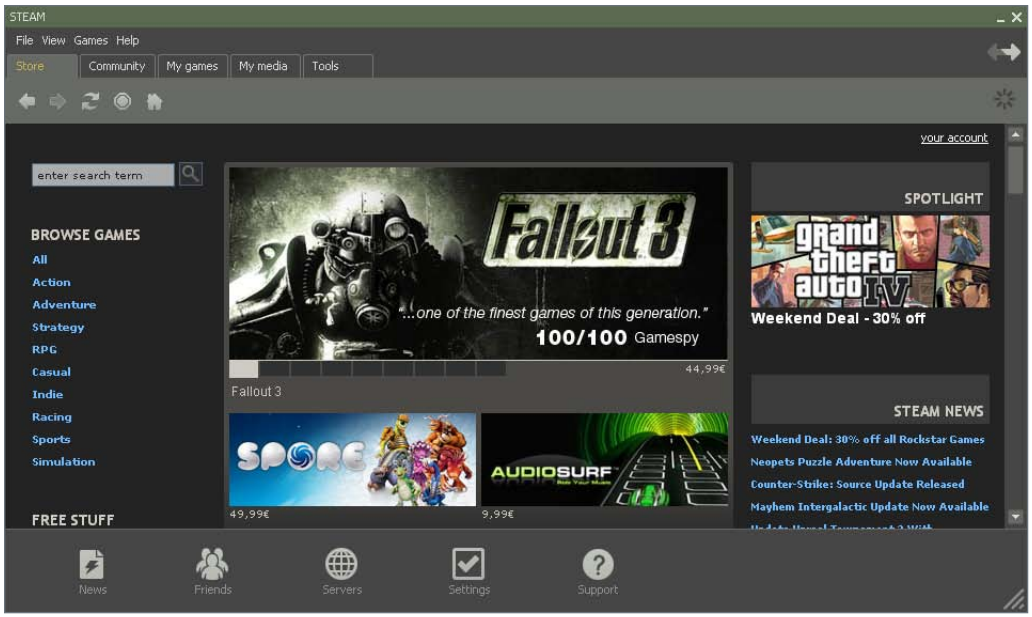

图 19：Steam 的在线商店。

```
if ( get_steam_install_path() && get_steam_installed_apps() )
{
  get_string_from_reg_key("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\", v0, HKEY_LOCAL_MACHINE, "ProductId");
  get_string_from_reg_key("SOFTWARE\\Microsoft\\Cryptography\\", v7, HKEY_LOCAL_MACHINE, "MachineGuid");
  get_string_from_reg_key("SOFTWARE\\Valve\\Half-Life\\Settings\\", v8, HKEY_CURRENT_USER, "io");
  lstrcpyA(&String1, "\n\r\n\r **********************************************\n\r");
  lstrcatA(&String1, "\n\r *************STEAM PASS STEALER*************\n\r");
```

图 20：Steam Stealer 的反编译伪代码摘录。

一旦 Steam Stealer 开始运行，将立即加载一些模块，以开始收集 Firefox 中保存的密码、CD 密钥以及大量热门游戏和 Microsoft 产品的产品 ID。Steam Stealer 跟踪属于产品的注册表路径的预定义列表，并读取注册表中的值，其中包含攻击者搜寻的未加密凭据。一个明确以 Steam 凭据为目标的组件会读取和解码其中包含用户 Steam 帐户和密码的文件。该文件 (ClientRegistry.blob) 位于 Steam 的安装目录中。被盗凭据的列表将汇编到堆栈变量中，并保存到磁盘上单独的位置，准备随时将窃取的凭据发送给攻击者。

根据 Steam Stealer 嵌入的配置，恶意软件也可能窃取即时通讯软件、电子邮件帐户、局域网帐户和 FTP 帐户的凭据。遗憾的是，并不是所有凭据在保存到磁盘之前都会被其应用程序加密。但有些应用程序确实给恶意软件作者制造了一些麻烦，在此情况下，恶意软件作者会使用免费的密码恢复软件来破解加密的凭据。可以将 Steam Stealer 配置为收集所有内容，并通过电子邮件（使用单独的 SMTP 组件）将收集到的内容传回原址，或将收集到的内容上传到 FTP 服务器。

总结：网络犯罪分子们利用经济危机实施犯罪活动

2009 年 2 月初，美国联邦调查局发布了一份新闻稿[6]，向公众通报了当前频发的在家办公诈骗问题。因经济危机而意外失去工作的人们正在急切寻找新的就业机会，并且愿意接受可以得到的任何工作，这种急切的心情很容易使他们卷入网络犯罪的骗局之中。他们可能会充当“钱骡”(money mule)，在网络骗子的指使下非法转移通过密码窃取程序获取的资金。这些背负极大经济压力的受害者往往不了解或不关心洗钱背后的犯罪活动。然而，他们从事的这一行当却非常危险。相关部门可以对他们的银行转帐行为进行逆向操作，从而使洗钱者的帐户留下漏洞，因此，这些钱骡很可能已在网络犯罪调查机构的监视之中。

幸运的是，许多银行限制了向国外转帐的金额。但是，在“钱骡”的帮助下，这种转帐行为看起来就像是国内交易，因此常常能够逃避执法机关的调查。然而，由于洗钱者一般更容易暴露，因此常常成为联邦执法部门发现和起诉的对象，而真正的幕后黑手却可以逍遥法外。消费者应时刻保持警惕，不要轻易接受那些好得令人难以置信的工作机会，以免无意中卷入到犯罪活动中。

回到虚拟世界中，攻击者隐藏在他人受感染的主机背后，因为现在的代理不需要配备单独的二进制文件，它们已成为恶意软件的一部分。与洗钱者在现实世界中的情况类似，犯罪分子会使用其“拥有”主机的 IP 地址以匿名方式进行网络犯罪。尽管受害者已经被密码窃取程序折腾得焦头烂额，却还将面对另外的打击。当查出受害者的家用 PC 是恶意软件攻击的源头时，受害者可能因进行网络犯罪而被追究法律责任。由于攻击者能够通过完全侵入的系统远程毁坏受感染的系统，因此，消除自己的踪迹就像玩计算机鼠标点击游戏一样简单。受害者甚至连请法律专家追查恶意软件来源的机会都没有。

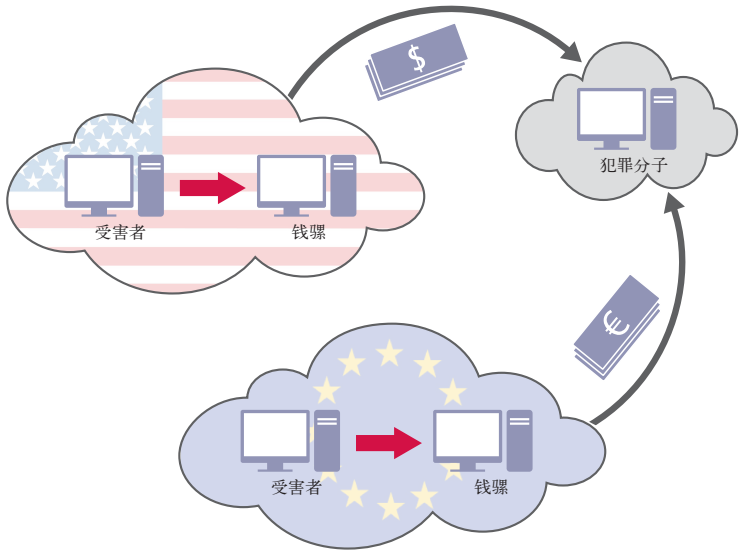

图 21：“钱骡”（洗钱中间人）和“在家办公诈骗”受害者参与犯罪活动的过程。

正如我们前文中所述，网络犯罪分子和网上银行机构之间的“警察抓小偷游戏”推动了密码窃取恶意软件的发展。但是，采用更多的安全措施并不一定能够带来更高的可用性。情况往往相反，对于用户而言，引入另一种安全机制常常使操作更为复杂，并最终使其放弃这一尝试。客户到底可以接受多高的复杂程度？输入或牢记另一个“秘密”代码显然不行。金融机构需要在安全性和可用性之间找到一个更好的折衷方法。有些消费者甚至会记下他们的 ATM PIN 号码并将其与银行卡一起放在钱包里，因为他们发现记住这么多代码和密码实在是一件困难的事情。毫无疑问，这样的行为会让所有的安全措施形同虚设。一次性密码令牌是一个良好的开端，但这些设备的成本却逐渐转嫁到客户身上。有多少用户愿意支付额外的银行安全费用（他们认为应该是免费的）？

6. http://www.fbi.gov/pressrel/pressrel09/workathomescams020309.htm。

可以肯定的是，密码窃取程序不会在短期内消失。随着易于使用的构建工具包的出现，只需单击鼠标，任何人都可以创建自定义的特洛伊木马程序，我们将面临密码窃取恶意软件日益复杂化的严酷现实。由于在线窃取凭据获利丰厚，犯罪分子绝不会轻易放手，而会将攻击目标扩大到银行客户和在线游戏玩家以外的用户。例如，侵入 ATM 操作系统和软件的“浏览”攻击就是一项可能在地下网络犯罪领域中普及的新技术。现在的恶意软件具有成熟的机制来规避安全解决方案并隐藏自己的踪迹，因此，当务之急不仅要阻止恶意软件，而且还要发现并隔离网络上现有的感染。固定网络流量出现增长或加密 HTTP 开机自我检测请求等奇怪行为都可能是受感染的迹象，并很容易被警报网络网关检测到。整个企业网络被一个员工感染的风险相当高：员工可能无意中将受感染的笔记本电脑或大容量存储设备带到工作场所并连接到企业网络。

在经济萧条时期，政府往往会采取一些保护主义措施并限制与其他国家/地区之间的贸易活动。但是，随着跨国界威胁（居住在一个国家的嫌疑人，在另一个国家进行犯罪活动）的出现，政府必须对网络犯罪活动给予更多的关注，并通过国际合作将犯罪分子绳之于法。

致谢

在此要特别感谢我们的同事 François Paget，他为我们提供了宝贵的统计数据。

关于作者

Dennis Elser 是迈克菲网关防恶意软件研发团队的高级工程师。他涉足的专业领域包括漏洞研究和前瞻性攻击检测技术的开发。Elser 是 McAfee Avert Labs 博客的固定撰稿人，并在 *Virus Bulletin* 杂志上发表过多篇文章，文章主题涵盖了从 Windows 漏洞到基于多媒体的恶意软件等多个方面。

Micha Pekrul 是迈克菲网关防恶意软件研发团队的高级工程师。他的专业领域包括恶意 Web 内容的研究，以及应用于迈克菲 Web 防恶意软件网关版中的相应检测方法的开发。Pekrul 经常在 Avert Labs 博客上分享他对于最新威胁的宝贵见解，并且在 *Virus Bulletin* 杂志上发表过多篇文章。

迈克菲（上海）软件有限公司

北京朝阳门外大街 16 号中国人寿大厦 1709 室　邮编：100020　电话：(8610) 85722000　传真：(8610) 85752299

上海市徐汇区虹桥路 3 号港汇 2 座 4005-4006 室　邮编：200030　电话：(8621) 61458878　传真：(8621) 61132278

广州市天河区体育东路 118 号财富广场西塔 15 楼 106 室　邮编：510620　电话：(8620) 38860668　传真：(8620) 38860638

销售热线：800-819-8879　*www.mcafee.com/cn*

McAfee、迈克菲和/或此处的其他标志均为 McAfee, Inc. 和/或其子公司在美国和/或其他国家或地区的注册商标或商标。与安全相关的 McAfee 红色是 McAfee 品牌产品的特有代表色。本文档中其他注册和未注册的所有商标均为其各自所有者专有。© 2009 McAfee, Inc. 保留所有权利。

6622wp_password-stealers_0709_ETMG