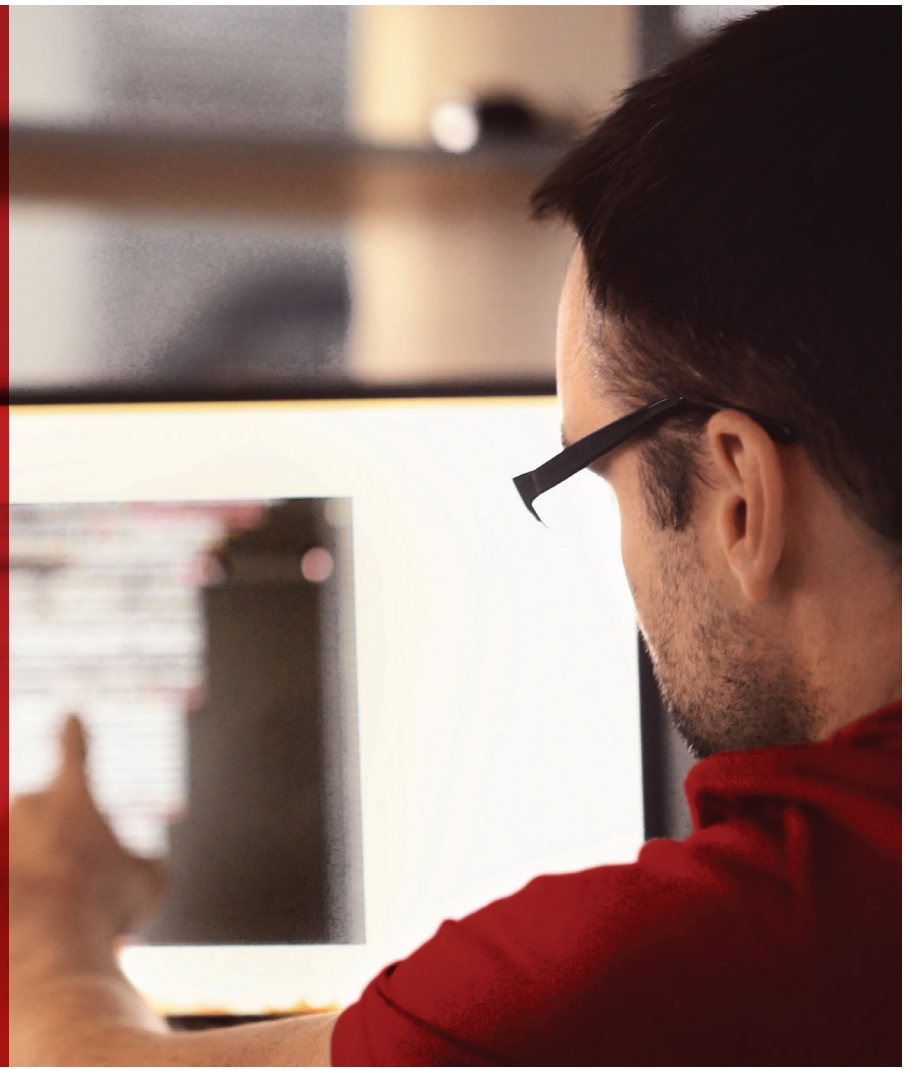
防范 Pinkslipbot

W32/Pinkslipbot 是一种自动繁殖的恶意程序系列，目的是为了窃取受害者的个人和财务数据。这种恶意软件可以通过基于命令的后门程序（由控制服务器运转）和基于虚拟网络计算的后门程序完全控制被感染的系统。Pinkslipbot 还可以通过网络共享传播到环境中的其他系统，并且可以与其控制服务器进行通信，以便下载自己的更新版本。



Pinkslipbot 最初在 2007 被发现，但是创建这个恶意程序的组织每隔几个月就会通过添加增量更新来维护代码库，然后将新的版本发布到网络上。

攻击者利用 Pinkslipbot 窃取的数据可以确定受感染系统的地理位置、所属组织以及所有者。攻击者可能会将此类信息（特别是来自著名组织的信息）倒卖给第三方，然后在获得付款后将针对性恶意软件部署到受害系统上。

要从技术方面深入了解 Pinkslipbot，请参阅《McAfee Labs 威胁报告：2016 年 6 月》。该报告讨论了初始感染过程、传播机制、技术细节以及常规预防技术。

防御 Pinkslipbot 的策略和步骤

下面是帮助您防范 Pinkslipbot 的一些常规策略和步骤。

为了保护外围入口的安全，您需要封锁所有网络入口点上不需要使用的端口，阻断往返于相关恶意 IP 地址之间的连接请求，并且禁止使用网络共享，这样才能防止 Pinkslipbot 的传播。在大多数环境下，您还需要禁用 Microsoft Windows 的 AutoRun（自动运行）功能。您必须将 Windows 操作系统和应用程序更新到最新的修补程序级别，还要将防恶意软件更新到最新版本。

未及时安装修补程序的系统往往存在易于被恶意软件利用的漏洞。对任何环境来说，完善的修补程序管理是必不可少的一项措施。一旦供应商发布修补程序，您就应该立即进行测试、验证和实施。如果由于早期版本的依赖性问题导致无法安装修补程序，则要采取其他措施来缓解对已知安全漏洞的利用。积极的修补程序管理机制是缓解 Pinkslipbot 和其他恶意软件影响的一种最有效方法。

虽然 Pinkslipbot 主要是在被漏洞利用工具包感染的网站上，通过随看随下的方式进行传播，但是受害者往往是被钓鱼电子邮件指引到这些网站的。通过将电子邮件标记为“内部”或“外部”，用户更容易识别伪造或钓鱼电子邮件，这样在点击未知的恶意链接之前就会慎之又慎。

Pinkslipbot 有一部分是在内存中运行，所以仅仅对系统进行修补还不足以应对，您还需要执行全盘扫描，再辅以恶意软件删除工具，才能将其清除。受感染的系统需要重启才能从内存中清除这种恶意软件，您最好再执行一次重新扫描，确保系统已经清理干净。我们还建议您使用复杂的强密码，防止遭到字典攻击，并且禁用“自动运行”功能，同时遵循仅授予“最低权限”的原则。

Pinkslipbot 是声名狼藉的 Zeus 特洛伊木马中极具攻击性的进化代表。如果使用简单的 Windows 系统登录密码，则会很容易被 Pinkslipbot 感染，它甚至不需要通过漏洞利用工具包或者用户交互来入侵您的系统。一旦系统被感染，它就会记录在系统上执行的一切活动，并且将收集的信息发送给攻击者。随着 Pinkslipbot 的控制服务器引入自定义的安全通信，您将会更加难以检测和分析这一款恶意软件。它过去的劣迹表明，随着它的不断迭代，其危险性会越来越强。通过了解您的环境并采用我们推荐的策略和步骤，您可以将 Pinkslipbot 可能会造成的损害降至最低。

McAfee 技术如何帮助防御 Pinkslipbot

McAfee VirusScan Enterprise (VSE) 和 McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise 和 McAfee Endpoint Security 10 为终端系统提供了先进的防恶意软件保护功能。McAfee VirusScan Enterprise 已经被 McAfee Endpoint Security 10 取代，后者在经过优化的平台上可以提供更高的性能。适用于 McAfee VirusScan Enterprise 的 McAfee DAT 和 McAfee Endpoint Security 10 包含检测和清除 Pinkslipbot 组件的功能。McAfee VirusScan Enterprise 和 McAfee Endpoint Security 10 通过内存检测、防 Rootkit、

行为分析和静态分析机制提供了多种防御级别。如果需要额外的防御层来应对新的变体，您可以实施访问保护规则，从而防止 Pinkslipbot 感染系统。

- 创建并测试访问保护规则，以阻止任何进程在 C:\Users*\AppData\Roaming\Microsoft**.exe 路径下执行和创建任何可执行文件。
- 创建并测试访问保护规则，以阻止 cscrpit.exe 和 wscript.exe 进程从 %LOCALAPPDATA%\Microsoft\ 文件夹读取、执行和创建 WPL 文件。这些文件通常是 JavaScript 文件。阻止这些文件可以防止恶意软件下载新的版本。
- 创建并测试访问保护规则，以阻止 cscrpit.exe 和 wscript.exe 进程从 %UserProfile% 文件夹读取和执行文件（如果可行）。
- 创建并测试访问保护规则，防止“updates_*new.cb”、“upd_*.cb”和“updates*_new.cb”执行和创建新文件。Pinkslipbot 的配置文件通常需要使用这些文件。阻止这些文件可以防止恶意软件更新。
- 对 iexplorer.exe 和 explorer.exe 进程的 65200 到 65400 端口创建并测试访问保护规则。因为 Pinkslipbot 会将自身注入这些进程，阻止用于防御 Pinkslipbot 与其控制服务器进行通信的进程使用这些端口。
- 实施并测试访问保护规则，以阻止远程执行 autorun.inf 文件。

McAfee Host Intrusion Prevention (HIPS)

McAfee Host Intrusion Prevention 通过结合使用特征码和行为入侵防护系统（具有动态的、有状态的防火墙），可防止系统遭受零日威胁入侵。定期更新内容以防止系统出现应用程序和操作系统漏洞，甚至在修补程序发布之前也可以提供保护。通过启用签名来防止恶意软件用来入侵常见软件的许多一般方法，从而加强环境的安全性。

- 测试并启用内置的 McAfee HIPS 特征码 6010 一般应用程序挂接保护。
- 测试并启用内置的 McAfee HIPS 特征码 6011 一般应用程序调用保护。
- 通过为被 Pinkslipbot 感染的系统分配一条防火墙策略，阻止除管理端口外的所有端口，从而将其隔离。

McAfee Endpoint Security 10 和 McAfee Host Intrusion Prevention 已随附在 McAfee Complete Endpoint Protection 中。

McAfee Web Gateway (MWG)

随看随下和电子邮件中的链接是 Pinkslipbot 用来进行传播的常见方法。McAfee Web Gateway 可以高效保护 Web 安全，防止系统被恶意网站入侵。它既可以作为专用硬件设备进行部署，也可以作为虚拟机映像进行部署。

- 配置 McAfee Web Gateway 以过滤垃圾邮件。
  - 垃圾邮件过滤可以防止：
    - 恶意 IP 地址
    - 恶意 URL
    - 垃圾电子邮件
- 启用 GAM 检查
- 启用 McAfee GTI 的 URL 和文件信誉功能。
- 与 McAfee Advanced Threat Defense 集成以实现沙盒和零日检测。

McAfee Active Response (MAR)

McAfee Active Response 可以为已被高级威胁（如 Pinkslipbot）盯住的系统提供持续的检测和响应服务。利用自动事件监控，您可以及时发现表明系统已被恶意软件感染的迹象。

- DNS 缓存中存在以下域名可能表明已遭到 Pinkslipbot 感染：
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- 执行以下 DNS 缓存查询可确定系统是否与上面列出的任何已知 Pinkslipbot 域名进行过通信。
  - DNSCache where DNSCache hostname equals “[Pinkslipbot 域名]”
- 此查询将返回从环境中的系统与 Pinkslipbot 域名建立过的通信的列表。通过点击列出的条目并显示相关的系统，您可以轻松判断出哪些系统在与这些域名进行通信。
- 利用本地防火墙（如 McAfee ENS 10 或 McAfee HIPS）可以隔离被 Pinkslipbot 感染的系统。要隔离系统，请在 McAfee ePO 中为相应的系统分配一条防火墙锁定策略。
- 通过在 McAfee ePO 中为系统指定“立即运行”“按需扫描任务”，运行完整的 McAfee ENS 10 或 McAfee VSE 按需扫描。唤醒代理以启动扫描。

延伸阅读

McAfee 恶意软件网络研讨会系列：Pinkslipbot

该视频提供了有关 Pinkslipbot、区域和行业细分、特征和症状，以及防范建议的概述。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn