Threat of the Month: 无文件恶意软件

无文件恶意软件是什么？

在每一场魔术表演中，舞台上的魔术师都会创造出某个令人称奇的幻象。观众的注意力集中在一个方向，而魔术师却在另一个方向暗中执行了一些戏法。无文件恶意软件也是如此；恶意攻击者通过将您引向错误的方向，让这种恶意软件偷偷越过您的防线。防病毒软件正在忙着扫描您的硬盘驱动器？这个狡猾的恶意软件系列在 RAM 中运行，无需将任何文件写入硬盘驱动器，因此您可以进行全面扫描，但却找不到任何破绽。同时，一个新的恶意软件已经从您的笔记本电脑建立了命令和控制通道。这种花招就好像魔术师从帽子里变出兔子一样不可信，在软件中，这就是恶意攻击。

您为何要关注此种威胁？

任何威胁，如果设计得足够复杂，就可以用来躲避某些类型的检测，都需要花时间来应对。无文件技术已存在一段时间，可用于隐藏现有的恶意软件。例如 **Kovter** 最初是勒索软件，之后的生命周期中通过垃圾邮件和恶意广告传播，最近被发现采用无文件恶意软件形式，躲避传统的检测。另一种备受关注的攻击来自 **DNS Messenger**，它会发起多阶段攻击，其中至少有一部分依赖于无文件恶意软件来躲避检测。最近的一个 DNS Messenger 攻击活动首先通过有针对性的鱼叉式网络钓鱼邮件进行伪装，使邮件看似是由美国证券交易委员会 (SEC) 发送的，借此提高可信度，诱使用户放心将其打开。这些邮件包含一个貌似官方的附件，如果打开该附件，会引发一系列复杂的活动，从而导致感染恶意软件。

无文件恶意软件如何工作？

无文件恶意软件是一种非常难以检测的、驻留在内存中的恶意软件，它可以从系统内存（而不是硬盘驱动器）运行，而无需创建任何文件。虽然所有活动都几乎不可能不留下任何痕迹，但通常无文件恶意软件几乎不会在硬盘上留下什么活动痕迹。根据攻击者的动机及其实现攻击目标的速度，驻留时间有所不同。除了驻留，由于这种类型的恶意软件在内存中运行，如果受害者计算机重新启动，系统会从内存中清除该恶意软件，同时也会清除任何对检测和发现攻击后进行取证分析有用的证据。

© 2018 思科和/或其附属公司。版权所有。

为什么需要重视此类攻击？

防病毒软件和其他终端技术会扫描文件以检测恶意或可疑代码。特别是，防病毒软件会查找与已知恶意文件匹配的综合特征。无文件恶意软件没有文件可供扫描或借以生成散列值以进行比较，因此可以躲避基于文件的安全技术，在用户网络环境中潜伏较长的时间。

延伸阅读

思科 Talos™ 团队：DNSMessenger
http://cs.co/9000DLppO

思科 Talos 团队：DNSMessenger 最新信息
http://cs.co/9005DLpVH

思科 AMP 演示：
http://cs.co/9008DLpTE

© 2018 思科和/或其附属公司。版权所有。思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。若要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

CXX-XXXXXX-00 09/18

我该怎么做？

要检测并阻止无文件恶意软件，您需要拓展防御策略，采用高级终端保护。攻击者会尝试任何技术组合来破坏您的网络，您需要做好随时防御的准备。对于 DNS Messenger，以及使用 DNS 攻击恶意互联网基础设施的许多恶意软件形式，DNS 层安全也是非常有效的方法。如果您采用分层的安全方法，使用有效的第一道防线（例如在 DNS 层）和有效的最后防线（除签名之外还采用其他策略的终端技术），则更有机会在魔术师消失在烟雾中并带走您的数据之前，弄清楚他们的魔术花招。

思科如何为您提供保护？

面向终端的高级恶意软件防护 (AMP)	利用内存保护和感染指标来检测无文件恶意软件，例如异常域名系统 (DNS) 通信和经过混淆处理的 Windows 注册表项。
思科邮件安全设备	检测并阻止网络钓鱼攻击
思科 Umbrella™	阻止命令和控制流量
下一代防火墙/ 下一代入侵防御系统/ 思科 Stealthwatch®	检测并阻止命令和控制流量等恶意流量、恶意软件传播尝试等。