安全

潜行匿迹：无文件恶意软件


Marc Blackmer
2018 年 9 月 13 日 - 3 条评论

我最近看到一则新闻，说有一项调查向受访者询问，他们是更希望拥有飞翔能力还是隐身能力。当然，这个问题非常不切实际*，但是听听受访者*如何选择*也很有意思。大多数人选择拥有飞翔能力。真正吸引我的是，该项调查的作者以为大多数人都会更希望拥有隐身能力。但是人们却选择了飞翔能力，因为他们将隐身能力与不道德的犯罪行为联系在了一起。

当然，这种联系让我想到了安全性。隐身是网络犯罪分子极力追求的目标，而无文件恶意软件的开发帮助他们越发接近这个目标。

无文件恶意软件是一种驻留在内存中的恶意软件。顾名思义，这种恶意软件在受害者的系统内存中运行，而不是在磁盘上的文件中运行。这导致它很难被检测出来，因为扫描不到任何文件。它使调查分析变得更加困难，因为当受害者的计算机重新启动时，这种恶意软件便会消失。

无文件恶意软件可以通过网络钓鱼、恶意网站等进入网络，就像任何其他类型的恶意软件一样。不同之处在于，它在实施感染时不会安装或运行任何可执行文件。这就是所谓的 “无文件” 的意思。然后，这种恶意软件会在系统内存中运行，并操纵管理实用程序（例如 Windows PowerShell 和 Windows Management Instrumentation [WMI]）来发起攻击。由于许多安全技术明确信任这些实用程序，因此这种恶意软件不易被发现，并且其活动会看似无害。

2017 年底，思科 Talos 威胁情报团队 发布了一篇博客文章，介绍一种名为 DNSMessenger 的新型无文件恶意软件。（您可以在此处全文阅读这篇有关 DNSMessenger 的博客文章）攻击者通过邮件向受害者发送受感染的 Word 文档，并诱使用户在文档中启用宏。启用后，宏便启动 Windows PowerShell 脚本，以通过 WMI 访问特定的互联网域。该恶意软件从与这些域关联的 DNS TXT 文件中收到进一步的指令。

以文件为中心的传统恶意软件检测技术无法检测到这种威胁，因为它不安装任何文件，并且将恶意指令巧妙地放置在受害者网络*外部*的 DNS 记录中。从基于文件的角度来看，一切都会显得很正常，必须密切监视 DNS 流量才能检测出这种威胁。

无文件恶意软件制作者使用的另一种技术是将编码命令放在一个或多个特定的 Windows 注册表项中。安全产品往往不会在注册表中查找恶意软件。注册表是受信任的位置。因此，如果 PowerShell 脚本读取注册表项，会发现该活动似乎并无异常。异常的是注册表项编码不正常。同样，基于文件的恶意软件检测不会检测到这种威胁，这就需要能够查找经过模糊处理的注册表项的终端保护技术。

这些只是几个示例，说明了攻击者会如何挖空心思利用可信进程和彼此孤立的安全技术之间的缺口。

攻击者不会只尝试一种攻击途径，未达到目标就放弃。他们会尝试各种途径，寻找一切可乘之机，利用漏洞在您的网络中获得落脚点。而前述安全保护技术方面的缺口就会让他们有机可乘。因此从逻辑上讲，仅通过一种安全技术无法防御所有这些变化多端的攻击。人们需要阻止网络钓鱼攻击；需要从邮件中删

除恶意附件；需要停止流向恶意域的流量；需要监视网络流量，以发现数据中心内外到终端的异常。当通过一种攻击途径检测到威胁时，需要在所有防御技术中共享该情报，最好通过自动化手段实现。

好消息是，我们可以实现这些目标，而且还可以提供更多优势。首先，我们制定了针对无文件恶意软件的感染指标，例如检测 DNS 请求中的异常内容或可用于混淆恶意命令的异常 Windows 注册表项内容。

接下来，我们从数千亿封邮件、超过 1000 亿条 DNS 请求中收集遥测数据，每天分析近 200 万个恶意软件样本。我们使用数千个蜜罐，通过恶意软件逆向工程和漏洞分析进行研究。由于我们的研究包括网络、终端、Web、云、邮件和文件，因此我们可以了解到更多内容并且可以检测到更多信息。我们的所有研究成果都会融入我们的整个安全产品组合，从而为您提供更好的保护。

如果您想了解有关无文件恶意软件的更多信息，请务必阅读上面链接的 Talos 博客文章以及此处的后续博客文章。这两篇博客文章的结尾都列出了我们帮助缓解无文件恶意软件威胁的方式。一如既往，我们很乐意通过即时在线演示或我们的安全专家提供的个性化演示与您分享我们的技术。

* 至于我吗？我会选择飞翔能力。不，是真的。

喜欢这些类型的文章？请订阅 Threat of the Month 博客系列，及时了解我们发现的新威胁。

标签:

- AMP
- 无文件恶意软件
- 恶意软件
- 安全
- 安全思想领袖
- Threat of the Month