

简译版

如何防御无文件恶意软件攻击

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	How to Defend Your Organization Against Fileless Malware Attacks		
原文作者	David Strom	原文发布日期	2019 年 4 月 17 日
作者简介	David Strom 是一位屡获殊荣的作家、编辑和在线通信专家，为众多初创公司和成熟的技术企业提供建议。 https://securityintelligence.com/author/david-strom/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/how-to-defend-your-organization-against-fileless-malware-attacks/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 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。 		

如何防御无文件恶意软件攻击

David Strom

2019 年 4 月 17 日

无文件恶意软件威胁及其对企业的潜在危害正在增长。

无文件恶意软件利用了攻击者称之为“靠山吃山”的方法，这意味着，它们使用的是 Windows 计算机上已经存在的代码。现代 Windows 计算机上有很多代码，例如 PowerShell、Windows Management Instrumentation(WMI)、Visual Basic(VB)、具有可操作数据的 Windows 注册表项、.NET 框架等等。恶意软件不必投放文件，就能够利用这些代码执行恶意活动。

将这些代码组合起来的策略称为“进程挖空”(process hollowing)，在该策略中，恶意软件将特定进程作为其代码的存储容器和传播机制。FireEye 公司最近发现的一起攻击就是将 PowerShell、VB 脚本和 .NET 组合在了一个软件包中。

利用 PowerShell 的攻击显著增加。去年秋，IBM X-Force 事件响应和情报服务团队(IRIS)展示了 PowerShell 漏洞利用代码的强大功能——代码直接从 PC 的内存中执行。此外，PowerShell 可用于执行远程访问攻击并绕过应用程序白名单保护。

面临这种不断增长的威胁，安全团队应该采取哪些防御措施呢？

保持全公司强大的安全态势

在对抗无文件恶意软件方面，最基本的措施是确保 Windows 计算机及时打补丁和更新。攻击者的一个方法是利用未打补丁的老旧系统，因此不及时打补丁会向企业网络引入漏洞。“永恒之蓝”(EternalBlue)的传播就很好地说明了这一点：早在该漏洞发布之前的一个月，补丁就已经发布了。

下一步是确保拥有可靠的安全意识培训方案。这并不是说年度演习或偶尔发送测试性网络钓鱼电子邮件。而是提出一个持续运作的计划，让用户意识到点击邮件附件和链接的风险。大多数无文件攻击都是从简单的钓鱼邮件开始的，因此企业应快速消除此类入口点，这非常重要。

第三步是了解内置 Windows 代码的行为，以便及时发现异常，例如安装加密 PowerShell

脚本并将其作为服务运行。加密和服务的结合使用应引起警惕。除了加密，攻击者有时也会使用压缩工具。另一个需要警惕的迹象是，PowerShell 脚本隐藏在TEMP 目录中。虽然从技术上看，这并不是无文件的，但这段代码很快就会转移到操作系统中更危险的部分。

了解访问权限

企业应该了解无文件恶意软件首次运行时会发生什么。如果企业的一位用户点击了恶意附件，恶意软件不一定会留在该用户的 PC 上。恶意软件的典型行为是，在网络中移动以寻找更有价值的目标，例如域控制器或 Web 服务器。为防止这种情况发生，企业应慎重分割网络，并了解用户的访问权限，尤其是第三方应用和用户的访问权限。

一种常见的攻击方法是，恶意软件边在网络中移动边提权——例如，攻击者可以使用 PowerShell 实现这一点。攻击者可以发出命令进行反向域名系统（DNS）查询，枚举任何网络共享上的访问控制列表并查找特定域组的成员。这意味着，对恶意软件的控制措施之一是限制管理员权限——将管理员权限限制在尽可能少的系统上。

许多无文件漏洞利用代码依赖于权限滥用（不再需要的权限或已离职雇员的权限）或过时的权限（用户不再使用该权限访问目标应用）。企业应该设计一种方法来快速检测和阻止这些情况的发生。企业还应禁用不需要的 Windows 程序。并非每个人都需要在他们的计算机上运行 PowerShell，或者支持.NET 框架。更有效的方法是，取消对诸如 SMBv1 等老旧协议的支持——正是该协议的漏洞成就了“魔窟”（WannaCry）。

最后，虽然 PowerShell 可以绕过应用程序白名单，但部署此类控件仍然是个好办法。企业越多地了解用户如何使用应用，就越有可能捕获到恶意软件（因为这些恶意软件会执行合法应用不执行的行为）。另一种方法是禁用宏，包括经常被恶意软件编写者滥用的 Office 宏，不过这不是一种通用解决方案，因为许多用户确实需要宏来办公。

另外，攻击者不仅针对 Windows 桌面计算机，有时也针对嵌入式 Windows POS 计算机。这类计算机的吸引力在于，它们可以直接访问支付卡数据，因此企业需要对这些计算机提供额外的保护。

协调对抗无文件恶意软件威胁

当无文件攻击日益猖獗时，微软并没有停滞不前。事实上，微软开发了一款名为“反恶

意软件扫描接口”（Antimalware Scan Interface, AMSI）的开放式接口。一些供应商已经开始使用该接口，能够更容易地检测无文件勒索软件的迹象，特别是在分析脚本行为方面。

此外，任何想要更好地了解无文件攻击的人，都应该了解开源项目 AltFS。这是一个完整的无文件虚拟文件系统，用于演示这些技术如何运作，并且可以部署在 Windows 和 Mac PC 上。

如上所述，对抗无文件恶意软件攻击需要下大力气，并协调各种工具和技术。随着更多不可预测的恶意软件威胁不断出现，企业应该采取措施来加强防御。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>