AhnLab

安全月刊

2020.10 Vol.95

Fileless Attack

© AhnLab, Inc. All rights reserved.

不留犯罪痕迹的无文件攻击正在增加

了解黑客的强大武器——无文件攻击

从几年前开始，“无文件（fileless）”一词经常出现在安全威胁报告和相关新闻中。全球信息安全企业趋势科技（Trend Micro）在去年发布的《2019中期安全威胁报告》宣布，与2018年同期相比，2019年上半年检测到的无文件攻击次数增加了265%以上。AhnLab也在今年初发表的《2020安全威胁展望》中预测，以无文件方式的目标型勒索软件攻击将正式开展攻势。安全行业的权威组织其预测的未来将持续增加的无文件攻击到底是什么?

本文介绍了无文件攻击的定义和演变。

无文件攻击是一种对系统造成损坏的攻击，在内存中运行执行恶意功能的代码。即使攻击者使用了无文件技术，但并表示在硬盘上没有留下任何内容。为了攻击的持续性（persistence），攻击者需要将恶意代码储存在存储设备中。但是，即使在这种情况下，攻击者也不会将其保存为我们熟知的可执行文件、脚本文件和文档文件等单个文件。也就是说，存储设备中并不存在文件类型的恶意代码。

无文件攻击的出现和发展

下面来简单了解一下无文件攻击的出现背景和攻击及防御技术的趋势。

[图1] 无文件攻击及防御技术的发展

在网络攻击技术中，也存在很多不使用恶意代码的攻击。尤其是，通过网络或 Web 进行的攻击在没有恶意代码的情况下通常是可能的。通过使用网络设备（例如防火墙、Web 防火墙、入侵检测系统（IDS））可以防御这种网络攻击。

如果攻击者无法通过网络直接访问，可能会选择通过电子邮件附件或互联网引入恶意文件。从防御的角度来看，会使用防病毒(Anti-virus) 软件来检测、拦截和删除这些恶意文件。防病毒软件主要处理文件。攻击者为了绕过防病毒软件检测，可能会使用各种方法，其中之一就是利用无文件技术的恶意代码。

即使防病毒软件没有检测到恶意代码，威胁分析人员也可以利用取证（forensic）技术，找出进一步的威胁或掌握攻击者的流入路径等攻击信息。攻击者则为了逃避使用取证技术的追踪，会尽可能地删除痕迹。攻击者的这种行为被称为反取证（Anti-forensic）。

由于分析文件或系统上的痕迹变得越来越难，从 2015 年左右开始，安全市场上开始出现了专注于恶意行为而非恶意文件的 EDR（端点检测和响应）类型的产品。

无文件攻击成为热门话题的原因

无文件攻击并非是最近出现的攻击技术，但最近为什么如此热门?

首先是，自从将 PowerShell 用于无文件攻击以来，它已扩展到 APT（高级持续性威胁）攻击和诸如勒索软件和加密货币挖矿的恶意代码的传播。尤其是，公开了许多具有基于 PowerShell 的无文件攻击功能的攻击模拟工具，因此在使用技术相对容易。在最近发生的入侵事件中，发现了很多使用该工具的痕迹。

其次是，无文件攻击起到了端点安全市场的“游戏规则改变者”的作用。由于针对文件的现有安全解决方案很难检测到无文件恶意代码，因此可以认为，无文件恶意代码促进了为解决这一问题而出现的 EDR 市场的形成和发展。

什么是高级挥发性威胁（Advanced Volatile Threat，AVT）?

读者们对“APT 攻击”应该已经很熟悉了。翻译成中文就是“智能型（高级）持续性威胁”。最近在 APT 攻击导致的入侵事件中，发现了很多无文件攻击，因此也将 APT 称为 AVT，即智能型（高级）挥发性威胁（Advanced Volatile Threat）。

AVT 攻击采用的是无文件攻击技术，攻击者使用只在内存中运行的内存恶意软件（in-memory malware）和 LOL 工具，尽量避免在目标系统中留下恶意痕迹。LOL 工具是意为自给自足的英文“Living Off The Land”的缩写。可以理解为，攻击者在攻击过程中使用目标系统内的常规工具，而是外部工具。

无文件攻击将数据保存在哪里?

攻击者可以根据需要执行攻击而不会在磁盘上留下任何攻击数据。此时，恶意代码只存在于内存中。但是，在这种情况下，重启系统后，所有的恶意代码都将消失，必须再次执行攻击才能获得目标系统的控制权。这对攻击者而言是一种负担。除特殊情况外，攻击者选择这种战略的情况并不多见。

因此，大部分攻击者会选择持续（persistence）战略，即使重启目标系统，恶意代码也能够继续运行，并且可以保持控制器。为此，将最少的恶意代码留在系统中，此时首选的位置是 等操作系统提供的领域 ，例如注册表、服务、任务计划、Windows 管理规范（Windows Management Instrumentation，WMI）。此外，虽然不是很普遍，但也可以储存在与用户应用程序的数据库相同位置，还可以储存在磁盘文件系统外部、未使用的闲置区域以及 OSD 管理区域之外的 HDD 固件。

攻击者为什么要使用无文件技术?

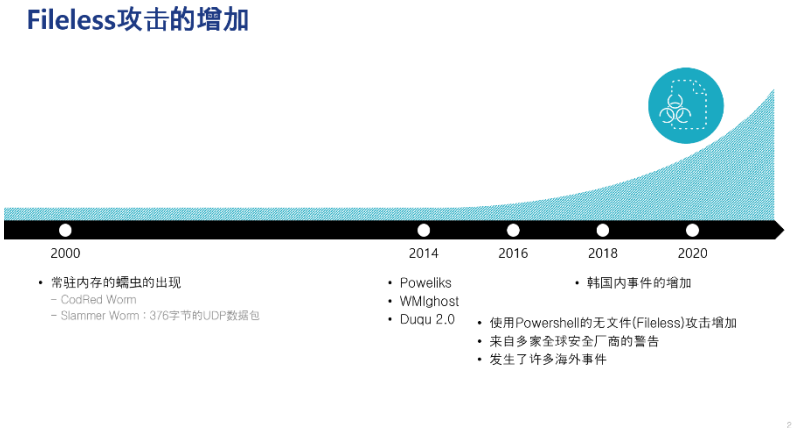
攻击者使用无文件技术，是因为不希望自己的攻击被检测或追踪到。

首先，从逃避检测的角度来看，如果攻击者引入的恶意代码在磁盘上不以文件形式存在，则不会被监控文件的防病毒软件检测到，因为没有扫描对象。另外，在仅允许运行白名单进程的安全解决方案中，如果将无文件技术与 LOL 工具一起使用，则有可能认为它是正常的，因此可以在不受限制地运行。

其次，从逃避追踪的角度来看，如果没有要由安全负责人检查的文件，则无法获取文件哈希值。那么，当您从 Virus Total 之类的网站上查找威胁情报时，您会怎么做？由于用于识别和判断恶意代码或攻击者的信息不足，因此对攻击者来说，不使用恶意文件是有利的。攻击者尝试避免将与攻击有关的信息保存到磁盘。如果已储存，则会通过完全删除等方式删除可能被追踪到的线索。

无文件攻击的出现和增加

如前所述，无攻击文件并非是最近出现的技术。2000 年代初期，也存在过驻留内存的恶意代码，之后又陆续出现了类似的恶意代码。在 2016 年，随着使用 PowerShell，无文件攻击开始呈现出增加趋势。在韩国，从 2018 年起开始发生了使用基于 PowerShell 的无文件技术的入侵事件。



[图2] 各年度无文件攻击的变化

使用无文件技术的攻击组

在MITRE ATT&CK中，无文件技术未分类为其他战术（tactic）或技术（technique）。但是，可以通过使用PowerShell或相关工具来识别确定为使用无文件技术的攻击组。MITRE ATT&CK分析各安全公司、公共机构和个人发行的公开报告和数据，总结并公开有关已知攻击组的信息。MITRE ATT&CK分析94个攻击组的结果，估计大约40%（35个）使用无文件技术。

admin@338, APT1, APT3, APT12, APT16, APT17, APT18, APT19, APT28, APT29, APT30, APT32, APT33, APT37, APT38, APT39, APT41, Axiom, BlackOasis, BRONZE BUTLER, Carbanak, Charming Kitten, Cleaver, Cobalt Group, CopyKittens, Dark Caracal, Darkhotel, DarkHydrus, Deep Panda, Dragonfly, Dragonfly 2.0, DragonOK, Dust Storm, Elderwood, Equation, FIN10, FIN4, FIN5, FIN6, FIN7, FIN8, Gallmaker, Gamaredon Group, GCMAN, Gorgon Group, Group5, Honeybee, Ke3chang, Kimsuky, Lazarus Group, Leafminer, Leviathan, Lotus Blossom, Machete, Magic Hound, menuPass, Moafee, Molerats, MuddyWater, Naikon, NEODYMIUM, Night Dragon, OilRig, Orangeworm, Patchwork, PittyTiger, PLATINUM, Poseidon Group, PROMETHIUM, Putter Panda, Rancor, RTM, Sandworm Team, Scarlet Mimic, Silence, SilverTerrier, Soft Cell, Sowbug, Stealth Falcon, Stolen Pencil, Strider, Suckfly, TA459, TA505, Taidoor, TEMP.Veles, The White Company, Threat Group-1314, Threat Group-3390, Thrip, Tropic Trooper, Turla, Winnti Group, WIRTE

[图3] 估计使用无文件技术的攻击组

使用基于PowerShell的无文件技术的主要攻击事例

2016年美国DNC（民主党全国委员会）被黑客攻击

在 2016 年美国总体大选期间，发生了被推测为系来自俄罗斯的攻击者攻击民主党相关组织的事件。 在这一事件中，攻击者使用了在 WMI 上注册 PowerShell One-liner 的技术。关于 PowerShell One-liner 的详细内容，将在后面进行说明。
当时，美国安全公司 Crowdstrike 进行了为期两周的取证分析后公布了结果，但关于攻击者是谁的法律层面的攻防仍在进行中。

2017年，全球40个国家的140个组织遭到黑客攻击

卡巴斯基在 2017 年发布了一份报告，报告称，全球 40 个国家/地区的约 140 个组织（包括政府、金融和通信）遭到了类似技术的攻击。该攻击使用了一种将 PowerShell One-liner 注册到注册表和服务的方法。

2018年~现在：勒索软件分发方式的变化

以前，知名的勒索软件通过偷渡式下载（Drive-By-Download）、伪装成正常软件和电子邮件附件等方式进行传播，但从 2018 年开始，它们开始使用无文件技术进行传播。AhnLab 通过 ASEC 博客发布的勒索软件的变化趋势如下：

发布日	标题
2018-04-17	以无文件形式传播的GandCrab v2.1
2018-06-05	无文件形式的Magniber勒索软件再次出现
2018-07-06	使用PowerShell脚本传播的GandCrab勒索软件（无文件）
2018-08-29	存在于Java脚本中的GandCrab勒索软件（诱导删除V3）
2018-09-03	使用PowerShell传播的GandCrab v4.4(Kill-Switch)
2018-10-01	使用WMIC删除V3 Lite功能的GandCrab v5.0.1的登场
2018-10-29	请注意！无法恢复的GandCrab v5.0.4正在在韩国传播
2018-11-16	请注意！SEON勒索软件（无文件形式）
2019-09-06	以无文件形式运行的WannaMine（SMB漏洞）
2019-12-03	具有SMB传播功能的Lemon_Duck恶意代码的传播
2019-12-17	V3的行为检测功能检测到无文件形式的BlueKeep漏洞的视频
2019-10-11	[注意] 以文件形式传播的Emotet恶意代码
2020-02-14	V3的行为检测功能检测IE漏洞（CVE-2019-1367）（无文件形式）

[表1] 勒索软件变化趋势

2019年，韩国大企业感染MyKings僵尸网络

在 2019 年，韩国某一大企业被一种名为 MyKings 的僵尸网络感染。攻击者的目的是运行加密货币挖矿恶意代码（CoinMiner）。攻击者利用了永恒之蓝（EternalBlue）漏洞感染了多个系统，并将 PowerShell One-liner 注册到任务计划和服务。

2019年，CLOP勒索软件感染

去年，韩国有 400 多个组织感染了 CLOP 勒索软件，这一事件引起了安全行业的关注。CLOP 勒索软件攻击是高级持续性威胁（APT）和勒索软件的组合。攻击者使用了一种称为 Cobalt Strike 的攻击模拟工具，从无文件的观点来看，使用了将 PowerShell One-liner 注册为服务的技术。

有效的防御需要卓越的解决方案和防御者的自主努力

自 2016 年以来，利用 PowerShell 的无文件技术被用作 APT 攻击或恶意代码分发等控制 Windows 系统的有效方法。攻击者可以运行仅在内存中运行的恶意代码，而该代码仅需一个大约 200 字节的 PowerShell One-liner。另外，为了持续保持控制权，有时还会配置后门程序或以非文件的方式将 PowerShell One-liner 储存在磁盘上。

由于无文件攻击不使用文件，所以通过一般的防病毒软件很难响应。为了了解攻击者的行为，需要加强系统的日志记录，并持续对其进行检查。由于攻击者的行为正在以难以明确判断是否是恶意的方式逐渐发展，因此从这一观点上，可以判断使用 EDR 解决方案是适当的选择。

攻击者总是能找到迂回现有防御系统的方法。为了阻止这些攻击者，还在不断开发防御系统，例如添加新的检测技术、提高响应方法等。但是，攻击和防御的战争不会结束。为了克服攻击技术和防御技术之间的时间差，防御者不应只依赖于安全解决方案，而要自主地努力关注新的攻击技术。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com
© 2020 AhnLab, Inc. All rights reserved.