安天智甲有效阻断 MedusaLocker 勒索软件变种

近日，安天 CERT 在梳理网络安全事件时发现一个名为 MedusaLocker 勒索软件变种，该勒索软件首次出现于 2019 年 9 月，主要通过垃圾邮件进行传播。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 MedusaLocker 勒索软件的加密行为。

MedusaLocker 勒索软件运行后将自身复制到 %APPDATA%\Roaming\ 目录下，并开始加密计算机上的文件，在被加密文件原文件名后追加名为“Readinstructions”的后缀。MedusaLocker 在计算机桌面上创建名为“HOW_TO_RECOVER_DATA.html”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 USER_ID 等。

▲MedusaLocker 勒索信

MedusaLocker 勒索软件采用 AES+RSA 加密算法，MedusaLocker 为防止受害者恢复已加密的文件，该勒索软件采取删除卷影副本、禁用修复、删除本地计算机的备份目录等行为。目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天智甲和安天追影已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、YARA 自定义鉴定器、动态行为鉴定器、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	269.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	338 KB
MD5	3EA4DFE71D3BDB4B0A5B0D472433628A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Script.AGeneric
判定依据	Trojan/Win32.Kryptik

◆ 操作系统

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★
获取系统版本	★
创建窗口	★
枚举进程	★
创建挂起进程	★★
自我复制	★★
访问文件尾部	★
获取驱动器类型	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
查找指定内核模块	★
文档篡改	★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 7 月 20 日 (总第 239 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼 II
威胁框架在智甲中的落地实践

智甲终端防御系统是面向政企单位的终端综合安全防护软件，产品依托于安天自主研发的下一代威胁检测引擎，集病毒查杀、实时防护、勒索病毒 / 挖矿病毒防护、漏洞检测与修复、终端管理、主机防火墙、外设管控、EDR、资产管理、主机加固、文件分析、威胁处置等多种功能于一体，可以为办公机、服务器、移动设备、虚拟化终端提供多层次、全周期的动态防护能力，实现终端安全统一管理、威胁事件统一处置、安全数据统一展示。

安天率先将 ATT&CK 威胁框架应用到终端产品的研发与能力验证工作中，不仅使产品在病毒攻击防御和异常事件捕获方面的能力大幅度提升，还可以支持以 ATT&CK 框架形式展现网内威胁事件，并能对事件进行关联分析。

威胁框架在端点防护中的价值

端点是威胁对抗的主战场，也是最后一道防线。据统计，绝大多数攻击技术与端点密切相关。传统的检测方式主要是针对单终端、单文件，而通过 ATT&CK 框架我们可以看出，很多攻击手段是复合的、多载荷的。因此，优秀的端点防护产品在面对装备最为精良、火力最为密集的攻击时，需具有以下能力：

1. 具有合理的架构安全体系，能够增强端点基础安全能力，以减少被攻击面；
2. 具有足够纵深的主动防御能力，能够在多个环节逐步抵消威胁；
3. 具有全面的信息采集与分析能力，以便发现常规防御手段无法发现的威胁。

当前终端防护产品有两大方向，一是以杀毒为基础，以防御病毒攻击为主；二是以 EDR 技术为基础，以捕获并分析异常事件为主。而各自的短板在实际场景中也日益凸显。

传统杀毒软件往往强主防、弱采集，几乎无法感知利用系统白文件的常规操作、或是利用某些 0day 漏洞所进行的攻击。传统杀毒软件没有将防御动作作为数据进行采集和记录，这样的设计导向使其主防能力并没有发挥最大效果。

而 EDR 类软件则重采集、轻主防，例如面对一些隐藏进程的攻击，没有强主防技术基础的 EDR 基本上是无法发现的。EDR 产品多数是基于应用层信息的提取，无法获取系统级、驱动层的信息，但往往这些数据才是支撑威胁分析和画像最重要的依据。

因此，在端点防护中，如果能把主动防御和数据采集两种能力相结合，则不仅能通过攻击动作发现威胁，还可以对整个攻击过程进行回溯，而引入 ATT&CK 威胁框架无疑是现阶段效果较好的一种选择。ATT&CK 可以帮助安全厂商对端点威胁有更深入的认知，由单载荷、单环节的层面提升到多个战术环节、多种攻击技术的层面，由被动防守的视角转变为以攻击者的视角去理解威胁，使防御体系的构建更具有主动性；ATT&CK 还能够指导产品构建清晰、完备的采集体系，其相对统一的定义也有助于分析人员快速准确、低成本的进行威胁分析和协同工作。

2019 年，安天将 ATT&CK 威胁框架作为安全产品开发的可落地的参考、及产品能力验证指标之一。为使 ATT&CK 更好地落地，采用主动防御能力作为基础的方式，在广度上基于常见威胁完善产品主防和采集点在 ATT&CK 中的覆盖度，基于新兴威胁补充 ATT&CK 的技术点，并可灵活配置以适配不同场景；同时，在深度上进一步挖掘单点的防御规则和采集方法，使产品能够提供更多行为动作、安全级别、告警级别、标签信息、行为信息等内容，提高对单点威胁的防护和感知能力。

威胁框架在智甲中的落地实践

智甲终端防御系统通过引入 ATT&CK 威胁框架，极大提升了主动防御能力和数据采集能力。

在主动防御能力方面，智甲首先基于对震网、方程式等重大威胁事件的分析，将其中病毒样本的攻击行为映射到 ATT&CK 中，从而筛选出攻击者常用的技术手段；其次，考虑到对终端正常业务的影响，针对每个技术点划分其对应的危害等级，并用红、黄、绿加以区分。红色表示相对危险的操作，这种操作的影响范围大，一旦在系统中发现，立即进行告警和拦截；黄色表示相对敏感的操作，对于这种操作无法一键报警，而是提醒用户，让用户选择是否拦截或做其他处理；绿色表示相对常规的操作，单独出现基本无危害，但是它有可能辅助恶意代码或威胁去做一些侦查、持久化的工作，因此采用仅采集和记录的处理方式。

▲安天智甲终端防御系统威胁框架能力映射图谱 (2019)

（下转第三版）

每周安全事件

类 型	内 容
中文标题	研究人员发现多功能木马 M00nD3V Logger
英文标题	Deep Dive Into the M00nD3V Logger
作者及单位	Rohit Chaturvedi&Naveen Selvan
内容概述	ThreatLabZ 观察到一个名为 M00nD3V Logger 的多功能信息窃取木马，其正在被一个多级加载器投送。由于具有多种窃取功能，M00nD3V Logger 逐渐在黑客论坛上流行起来。M00nD3V Logger 通过带有 zip 附件的垃圾邮件或受感染网站将有效载荷投送到受害者的机器上。M00nD3V Logger 除了窃取信息外，还配备了其它主要功能，包括反僵尸软件、杀毒软件、通过 SMTP/FTP/ 代理进行通信、下载额外的插件以及 BouncyCastle 加密包。
链接地址	https://www.zscaler.com/blogs/research/deep-dive-m00nd3v-logger

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft Internet Explorer、Edge 和 ChakraCore 安全漏洞（CVE-2020-1219）	高	Microsoft 浏览器访问内存中对象的方式中存在远程代码执行漏洞。此漏洞可能以一种允许攻击者在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	Microsoft Windows Shell 安全漏洞（CVE-2020-1286）	高	当 Windows Shell 不正确地验证文件路径时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有提升特权的新帐户。
	Microsoft Internet Explorer VBScript Engine 安全漏洞（CVE-2020-1213）	高	VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
较为活跃样本家族	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan/Win32.Patched	中	此威胁是一种窃密类木马家族。该家族木马运行后，打开 IE 浏览器，并将木马中的 shellcode 读到内存中并执行，具体操作为记录 WINDOWS 登陆账户信息，试图窃取 SQL 账号密码信息，以 URL 方式发送到作者服务器中。
	Trojan/Win32.Autoit	中	此威胁是一种由 Autoit 脚本编写的木马家族。该家族木马具有多种功能，可以窃取用户信息、接受远程控制、下载并安装其它恶意代码等。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan[Backdoor]/Linux.Gafgyt	中	此威胁是 Linux 平台上的具有窃密行为的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作，并且会收集机器上的信息上传给远程控制端。
	Trojan/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。
	Trojan[Clicker]/Android.Simpo	低	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成其他正常应用，运行后隐藏图标，并访问某些网站，旨在提高网络访问流量，消耗用户流量资费。

（上接第一版）

虽然，病毒样本在攻击过程中所涉及到的动作都可对应到 ATT&CK 的技术点上，但是 ATT&CK 针对这些技术点提供的防御方法和缓解措施也并不是非常全面的。智甲针对 ATT&CK 中没有给出具体防护实例的项目，基于实际样本分析，逐条补充了防护规则。例如，攻击者使用钓鱼邮件进行攻击，ATT&CK 仅描述了防护思路，并没有给出具体的防护方法，而智甲通过对邮件正文进行监控，判断接收附件是否存在敏感词汇、诱饵名称、钓鱼链接、钓鱼附件的防御规则实现邮件监控；同时，对于防护方式不足的重点项目，智甲也做了相应的补充。例如，攻击者创建系统服务实现持久化并释放 rootkit 驱动，实现隐藏文件、进程和服务，ATT&CK 仅使用命令行参数执行防护，而智甲通过检测是否存在危险行为，包括非法第三方应用建立服务和驱动、修改 PE 文件属性为隐藏、进程隐藏等防御规则实现注册表监控、文件监控、进程监控。

除此之外，智甲在 ATT&CK 的基础上，将防御重点放在事中防御和事后防御，进一步提升主防能力。例如，某些恶意代码会将执行体写入正常进程的内存中（通常是系统程序或者常见的应用程序），以此实现绕过主动防御或者 EDR 产品的数据采集与监控。ATT&CK 将其定义为 Process Hollowing 技术，但认为该类攻击无法通过事前预防性控制来缓解。基于此指引，智甲防御策略如下：

防御策略 1（事中防御）：通过数据采集功能监测 CreateProcess 事件的详情，并同时监控多个与之相关的 API 调用情况，在发现内存篡改行为后立即进行拦截和告警；

防御策略 2（事后防御）：如果在安装系统前用户终端已遭到该类攻击，可以在安装系统后对所有存活进程的内存进行扫描，并将该内存与存储在磁盘中的实体进行匹配，当发现内容不匹配后，会主动分析其不匹配原因，查看是否挂钩或者进行相应的内存修改，如果发现恶意代码会主动结束恶意程序的执行。

在数据采集能力方面，防御和采集是一体的，所有主防的防御动作都可以根据配置决定是否记录。并且，ATT&CK 在端点数据采集能力上的优势是不容忽视的，ATT&CK 可作为攻击事件的回溯依据，更全面的记录端点环境变更历史，也能更好的理解对手的 TTPs；ATT&CK 可聚焦更重要的数据，针对攻击手段可能留下的数据痕迹进行专项采集，也可针对系统组件被恶意利用加强数据采集；ATT&CK 可为态势感知提供数据支持，更好的进行分析威胁和威胁研判。

基于 ATT&CK 技术点中的数据源，智甲的采集点划分为既有、新增、额外，尚未覆盖四部分。智甲目前已有的采集能力，包括进程监控、MBR 信息、邮件监控、Windows 注册表、系统日志等与 ATT&CK 相匹配。目前在 ATT&CK 指引下，智甲又新增了进程命令行参数、利用防病毒、命名管道、密钥文件访问日志等采集能力，而对于 ATT&CK 中没有涉及到的 WiFi 连接信息、漏洞信息、账号与口令、USB 设备使用等采集能力，智甲也是具有的。

除此之外，智甲针对不同场景配置不同的数据采集策略。在日常监控场景下，重点监控关键项目，并采用产品默认采集范围的采集方式；在重点蹲守场景下，除常规项目外，要更多的关注内存发现异常 HOOK、系统 API 调用等，采集方式倾向于针对特定范围端点进行全要素采集；在处置追溯场景下，主要采集特定文件传播情况，或者网络流向情况等横向传播环节相关数据进行采集，采用自定义规则、按需采集采集方式。

截至 2020 年 4 月份，ATT&CK 威胁框架把威胁过程分为 464 小项，其中可防御 134 项，且智甲基于现有能力已实现 97 项；可检测 108 项，已实现 52 项。

实践中的经验与反思

▲遭受钓鱼邮件攻击时的防御过程

上图是智甲融合威胁框架后，受到钓鱼邮件攻击时的整个防御过程。智甲如果仅仅是基于特征库的扫描和进程监控，而病毒做了免杀且通过 PowerShell 和 CMD 调用，则智甲很可能就无法检测。而智甲融合威胁框架后，增强了在各种环节的采集和感知能力，基于这些采集到的信息（红色部分），可以快速准确的发现威胁。

基于上述实践，智甲对于 ATT&CK 威胁框架的落地形成了一些经验总结。第一，ATT&CK 不能仅用于对分析报表的丰富，要避免成为当年“初代”态势感知只有“地图炮”的情况；第二，安全产品更多需要具有原生的主防和采集能力，而不要过度依赖第三方工具。如果过于依赖 Sysmon 等第三方监控工具，既没有完成产品自身能力的闭环，也对威胁情报等安全资源利用效率造成障碍；工具类（仍以 Sysmon 为例）的不可持续性不适合企业级常态化监控场景，其配置的复杂度也不具备在规模化端点环境下的实施条件。

长远来看，ATT&CK 中针对端点的攻击手段占据了较大比重，端点则是网络攻防战中的主战场。尤其是在面对高威胁对抗的网络攻击时，边界侧的防护能力正在逐渐失效，因此未来应当在端点侧投入更多努力以提升主动防御和数据采集能力。

威胁框架使我们对端点主动防御和数据采集的能力指标有了更清晰认知和衡量标准。我们可以通过威胁框架去检验端点防御能力和采集范围的有效性，并加以完善。同时，威胁框架亦非端点检测技术的全部，我们需要持续探究现有威胁框架没有覆盖的攻击手段：

- 在广度上不断提升在各个攻击环节的覆盖面
- 在深度上加深对各攻击点的研究与防护投入
- 探究如何落地才是适合国内环境的最佳实践

微信扫描二维码关注公众号查看原文