安天发布《Ako 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Ako 的勒索软件变种，该勒索软件最早于本月初被发现，主要通过垃圾邮件和 RDP 暴力破解进行传播。Ako 勒索软件已发现五次更新，各变种的不同主要在于勒索信中的版本信息。

Ako 勒索软件执行后，加密计算机上的文档文件，在原文件名后追加名为“.73BLn8”的后缀，在含有被加密文件的位置创建名为“ako-readme.txt”的勒索信和包含被加密的加密密钥的名为“id.key”文件，该勒索信内容包含勒索说明、Tor 浏览器下载地址、支付赎金的暗网地址、base64 编码的 USER_ID 和版本信息等。Ako 勒索软件使用“RSA+AES”加密算法加密文件，通过 ARP 协议扫描局域网主机，对存活主机进行探测，并对共享文件进行加密。调用命令行命令来防止受害者恢复文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。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口令；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，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、聚类分析鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器等鉴定分析。

最终依据动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	Ako.exe
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	819 KB
MD5	7DE0C15B0DA4F6BE8C32D8CDFB372CC5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为

◆ 操作系统

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
删除全盘所有卷影副本	★★★★
在启动时禁用 Windows 错误恢复	★★★★
查询系统硬盘大小	★★★
堆喷射	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取计算机名	★
检索系统内存信息	★
WMIC 调用执行	★★
获得计算机用户名	★
创建窗口	★
获取驱动器类型	★
扫描磁盘类型	★★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
访问文件尾部	★
.....	.....

◆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 1 月 20 日 (总第 217 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

威胁框架：艰难的落地实践—安天冬训营次日纪实

冬训营第二日，网络安全研究者和工程师继续围绕会议主题，从以威胁框架为方法框架分析安天历史上曝光的经典 APT 事件入手，介绍在智甲端点防御系统、探海威胁检测系统、追影威胁分析系统等产品通过威胁框架对标形成的新的能力特点，以及安天下一代威胁检测引擎、威胁情报生产体系等内核和支撑环节对威胁情报的支持情况。安天向参会嘉宾介绍了三款主机安全工具的研发思路和使用方法。

安天应急响应中心：震网与 SWIFT 入侵事件的对比回顾—超高能力网空威胁行为体的作业模式分析

网空威胁行为体是网络空间攻击活动的来源，它们有不同的目的和动机，其能力也存在明显的差异。根据作业动机、攻击能力、掌控资源等角度，安天结合与业内专家的研讨，将网空威胁行为体正式划分为七个层级，分别是业余黑客、黑产组织、网络犯罪团伙或黑客组织、网络恐怖组织、一般能力国家 / 地区行为体、高级能力国家 / 地区行为体、超高能力国家 / 地区行为体。其中，超高能力国家 / 地区行为体，或称为超高能力网空威胁行为体，拥有严密的规模建制，庞大的支撑工程体系，掌控体系化的攻击装备和攻击资源，可以进行最为隐蔽和致命的网络攻击。安天将这种网络攻击称之为 A²PT（高级的高级持续性威胁）。2019 年安天发布了两篇超高能力网空威胁行为体的长篇分析报告——《震网事件的九年再复盘与思考》和《“方程式组织”攻击中东 SWIFT 服务商事件复盘分析报告》。本次冬训营安天分析人员，以两篇报告为内容基础，进一步披露一些未公开的研究内容和更完整的攻击事件链细节，借助 TCTF 威胁框架，分析在体系化支撑下，针对隔离网目标的集成化武器作业与针对连接互联网基础设施目标展开远程推进式作业两种作业模式的异同。

安天态势感知研发部：从态势感知视角分析方程式攻击中东最大 SWIFT 服务商事件

本议题延续前一议题对“方程式”组织攻击中东 SWIFT 供应商事件（以下简称 SWIFT 事件）的复盘分析。按照威胁框架将整个攻击过程动作逐个进行精细化拆解，通过回放每个攻击分解步骤，分析每个攻击步骤中防御方在基础结构安全工作、防御纵深设置、事件采集与留存、系统配置策略、安全产品布防等方面的不足，在 A²PT 级别的攻击下，单点安全能力失效是难以避免的，需要把敌已在内作为基础的敌情想定，以面向失效的设计为基本规划原则。在“实战化”安全运行环境中检验和持续提升防御能力。以资产安全运维平台明晰资产底数，形成网空地形，建立统一安全补丁、统一安全策略分发调整，实现有效的资产安全加固。通过端点侧、网络侧、分析侧的有效数据采集、情报生产，建设态势感知平台系统进行数据汇聚和分析，形成有效安全策略，指控响应行动。安天正在研发的战术型态势感知平台，在安天全线产品体系支撑下通过全面监测和发现、自动化甄别与研判威胁，辅助资产安全运维，利用多源威胁情报和私有化生产的内部情报，赋能客户，协助客户开展网络安全防御体系的构建和防御能力的持续提升。

安天端点安全产品子线：威胁框架在端点主动防御和数据采集的应用 ——ATT&CK 在端点防护的实践分享

本议题主要从端点防护系统的主动防御和数据采集两个方面，介绍了安天智甲终端防御系统借助 ATT&CK 威胁框架提升防御和采集效果的实践经验。

传统杀毒软件重主防、轻采集，导致对态势判断画像的基础数据供给不足，未发挥出主防技术驱动层、内核级的工作机理优势；而新兴 EDR 软件重采集、弱主防，实际数据采集层次较浅，难以发现内核级安全事件。因此安天认为一款合格的端点防护产品，应该在主动防御和数据采集画像两个方面结合发力，而威胁框架对于提升和验证主动防御和数据采集能力具有较高价值。

通过回顾安天智甲终端防御系统应用 ATT&CK 威胁框架的实践过程，总结了 ATT&CK 在端点落地的经验和注意事项，例如技术点选取的优先级、如何针对 ATT&CK 官方实例给出的防御方法不充分的情况进行补充等。此外在数据采集方面，基于智甲采集能力在 ATT&CK 威胁框架中的映射，强调了 ATT&CK 对构建清晰、完备的采集体系的价值，以及在日常监控、重点蹲守、处置追溯等不同应用场景下数据采集的落地方案。

报告结合实际攻防场景，演示了智甲产品在融合了 ATT&CK 威胁框架后如何在攻击的每个环节进行拦截和信息采集，进而达成最终防护效果。同时强调了威胁框架落地的注意事项，例如不能只注重可视化效果而忽略在端点的防护能力，并指出在规模化信息资产防御场景中，需要具有全面自动化采集部署机制的端点防御产品、可落地的响应猎杀流程与机制以及能够和

（下转第三版）

尊敬的读者：
2020 年春节即将来临，《安天周观察》于春节期间休刊两期，恢复出版时间为 2020 年 2 月 10 日。
感谢所有读者对《安天周观察》一直以来的支持与关注！
祝大家春节快乐！
2002 年 1 月 20 日

每周安全事件

类 型	内 容
中文标题	不安全数据库暴露数千英国公民敏感信息
英文标题	An unsecured database exposed thousands of British passports
作者及单位	NICOLE KOBIE
内容概述	安全研究人员发现了一个不安全的 Amazon Web Services（AWS）S3 数据库，其暴露了数千英国公民敏感信息。该没有安全保护的数据库暴露的文件包括护照、税务文件、工作申请、地址证明、背景检查、费用表格、带有签名的完整合同扫描、工资信息、电子邮件等。这些文件包含个人身份信息，包括姓名、地址、电话号码、出生日期、性别、国家保险号码。研究人员发现这些与英国有关的数据可以追溯到 2011 年，但大多数是从 2014 年到 2015 年，并且与一系列人力资源相关的咨询公司有关，其中大多数已经倒闭。
链接地址	https://www.wired.co.uk/article/uk-passports-exposed-data-breach

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.SideWinder.a[prv,spy] 2020-01-12	高	该应用程序是一款间谍软件，运行后下载恶意子包，利用漏洞获取 root 权限，窃取用户地理位置、社交应用数据、相册、账号、截屏文件、安装包列表等隐私信息，并将用户隐私上传至服务器，造成用户隐私泄露，建议卸载。
		RiskWare/Android.SexApp.dl[rog,exp] 2020-01-13	低	该应用程序包含色情敏感内容，其内容可能影响用户身心健康，请注意提示信息，使用健康绿色软件。
		RiskWare/Android.Joke.n[rog] 2020-01-14	低	该应用程序是整蛊程序，运行调整音量到最大，播放指定音频文件，修改用户桌面壁纸，部分壁纸为色情图片，建议不要使用。
	较为活跃样本	Trojan/Android.jmelon.b[exp,rog]	中	该应用程序运行后会启动其他恶意程序，联网上传设备固件信息和安装应用列表信息，后台推送广告，造成用户资费消耗，建议不要使用。
		G-Ware/Android.HiddenAds.ke[exp,rog]	低	该应用程序安装后隐藏图标，包含广告插件，会推送各种类型的广告，可能造成用户资费消耗，建议卸载。
		Trojan/Android.SmsSend.px[exp]	低	该应用程序运行后激活设备管理器，私发短信，造成用户资费损耗，请卸载。
		G-Ware/Android.HiddenAds.jy[exp,rog]	低	该应用程序运行后隐藏图标，后台加载广告，造成用户的资费消耗，建议卸载。
		PornWare/Android.SexPay.m[exp,rog]	低	该应用程序运行后推送色情内容，诱导用户订购付费，会造成用户资费损耗，请使用绿色健康软件。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Win32k 图形组件远程代码执行漏洞（CVE-2019-1468）	高	当 Windows 字体库无法正确处理嵌入的字体时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者随后可安装程序；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。若要利用此漏洞，攻击者需要设计一个含有恶意代码的网站，然后诱使用户查看该网站。
	较为活跃样本	Trojan[Ransom]/Win32.PornoAsset	中	此威胁是一种劫持用户系统并索要赎金的木马类程序。黑客利用 PornoAsset 家族勒索用户来获利。勒索类的木马一般通过下载或系统漏洞等方式来感染用户系统。部分勒索木马对用户数据进行加密，用户只有支付赎金后才能解密数据；另一种勒索木马不采用加密方式，直接锁定用户的系统，用户支付赎金后才能将系统解锁。
		Trojan/Win32.Velodrag	中	此威胁是一种木马类程序。该家族通常与其他恶意软件捆绑在一起，被安装到用户电脑中；或是通过恶意网站下载到电脑中。该家族会将自己的恶意文件添加到系统文件夹中，同时删除其他系统文件。
		Trojan[Backdoor]/Win32.Buterat	中	此威胁是一种后门类木马程序。该家族会在系统中打开后门，并注入其他的木马家族或恶意软件。该家族还可以允许黑客远程连接被入侵的电脑。
		GrayWare[AdWare]/Win32.ScreenSaver	低	此威胁是一种广告类灰色软件程序。该家族运行后会弹出窗口，显示广告，占用系统资源，影响用户使用电脑。
		GrayWare[AdWare]/Win32.AdLoad	低	此威胁是一种具有推送广告行为的灰色软件类程序。该家族运行后，会在电脑中下载并安装其它程序，添加注册表以实现自启动，占用系统资源，影响用户使用电脑。

（上接第一版）

态势感知对接的商用级分析工具。

安天监测分析产品子线：流量全要素记录融合细粒度威胁情报支撑威胁猎杀

报告根据“敌将在内、敌已在内”的敌情想定，将“探海”威胁检测系统部署于攻击者的必经之路，基于合理设计的防御纵深，在充分考虑单点失效的前提下，保障交叉火力对威胁行为体的行为感知覆盖，同时也为分析人员全面掌握资产、实现实体分析提供全要素采集的支撑。“探海”提供的全要素采集能力借助较完备的元数据化技术，在保障威胁猎杀所需完整要素的前提下，比全流量记录更节约空间；“探海”也提供了情报和场景触发的不同粒度数据记录能力，特定条件下可记录全流量数据，辅助威胁分析并固化证据；提取的各种元数据不仅保障了对威胁框架中技术的感知能力覆盖，也为下一代引擎提供了丰富的输入对象，使得“探海”可以借助下一代引擎提供的丰富拆解能力、情报承载能力以及沙箱的动态分析能力，在一定程度上补足流量与终端行为之间的断链。

综合多种数据融合的能力，“探海”不仅提供了全要素的记录，更可以融合威胁情报基于确定的线索辅助人员完成组织同源的关联分析，可以根据情报指引、场景条件触发记录的不同粒度数据，进行分析并产出新线索。

为平衡对威胁感知的全方位覆盖和保障业务的连续可用，旁路部署流量检测设备对分光或镜像的流量进行检测和记录是建设动态综合防御体系的过程中经常使用的方案。流量全要素记录能力在威胁框架的指引下，融合了细粒度的威胁情报之后，可以获得相当优秀的威胁检测能力。安天的探海威胁检测系统与追影威胁分析系统的搭档组合，继在 2018 年取得中国网络威胁对抗赛的两项冠军之后，又获得了 2019 年该比赛的第一名，蝉联冠军，正是依靠了全要素记录能力与承载威胁情报的下一代威胁检测引擎。

融合威胁情报与威胁框架的技术实践，从 2019 年下半年开始，在客户探针部署中，为客户提供了有效的威胁猎杀指引，支撑了态势感知能力的建设，这些能力都将在今年走向更多客户。

安天基础引擎研发部：下一代威胁检测引擎承载威胁情报

“谁对我发起了攻击？用了什么手段？我面临什么样的威胁？我需要作出怎样的防御动作？我能够自动化的完成这些动作么？……”这些都是在新的网络安全形势下需要被解决的问题。

面对这样的需求，业界普遍引入威胁情报来解决这些问题。IOC 情报常常被与传统反病毒产品一起使用，人们期望这样能够达成对攻击方所使用的装备或基础设施的指向能力和对海量的恶意代码的检测与辨识能力，从而达到发现和阻断威胁的作用。这种检测能力组合虽然对类似海莲花、白象、绿斑一类的 APT 攻击具有一定的价值，但在过去十年内对于对抗来自更高水平的威胁行为体的活动收效甚微。在对类似毒曲 II、方程式等高级威胁行动或组织的发现、阻断和猎杀活动中，这些情报几乎无法发挥任何作用。这主要和 IOC 情报本身检测机制的鲁棒性较差以及传统反病毒引擎的局限性有关。

传统的威胁情报，能够较低成本有效落地使用的通常只有 Hash、域名、URL 等 IOC 信标，面对广泛使用不落地样本、样本按需定制和掌控大量 C2 基础设施的攻击方，传统威胁情报效用性不佳。而在威胁分析成果中，一些的事实上可机读、可形式化的信息，例如关键代码段、关键字符串等，因安全产品缺少足够的预处理能力，无法实现情报落地。在业内资深专家的指导下，安天下一代威胁检测引擎全面完善了情报承载能力，支持对多种形式化信息进行匹配，拓宽了用户扩展情报能力的“频谱”。

传统反病毒引擎配套提供的知识决策信息是单一病毒名，对于高级威胁对抗来说信息不足。安天下一代威胁检测引擎支持多种输入与输出，包括对应载荷的 ATT&CK 威胁框架、TCTF 威胁框架相关的知识映射标签。

安天研究院：打造一个轻量级分析工具

安天研究院研究人员介绍了安天轻量级行为分析工具产品行为显微镜（Action Scope）的研发过程和能力特点。并就如何推动研发体系和分析体系实现有效的能力协同分享了自己的思考。

会上，安天向现场嘉宾通过 U 盘发放了 3 个实用安全工具的免费版本，安天工程师介绍了研发思路和使用方法。

行为显微镜 Action Scope

Action Scope 是安天研究院研发的对程序的动态行为进行揭示的便携类工具产品，通过动态行为监控与人工交互分析的有效结合，揭示文件每一步执行的具体行为、模块调用及漏洞利用等情况，辅助专业分析人员进行判定。

系统深度分析工具 ATool

ATool 是安天面向威胁检测与威胁分析人员开发的 Windows 系统深度分析工具，其通过对系统内核模块、驱动、服务、进程、模块、端口等信息进行分析关联，进行对象的安全检查和可信验证，协助完成手动分析处置工作。该工具最早版本发布于 2002 年，并在 2006 年引入了四层守信模型进行安全分析，是安天威胁分析猎杀工程师的必备工具。

精细化扫描工具 ScanTool

ScanTool 是一款区别于传统病毒检测工具与计算机取证工具的便携式自动化检测工具，其核心是对主机全量文件和其他检测对象完成多引擎的检测扫描和全面的元数据提取与验证，形成完整日志，并提取出可疑文件。为专业分析人员快速定位威胁及取证工作提供有力支撑。

安天通过创意安天论坛（http://bbs.antiy.cn）对相关工具免费版本提供支持。

会议最后，安天研究院介绍了《Windows 的安全演进对国产操作系统的启示》。

随着网络强国战略的不断推进实施，网络安全所面临的风险挑战也会更加严峻，对能力型网络安全企业的使命要求也在不断提高。从与恶意代码对抗的小闭环，走向全面赋能客户、助力客户建设防御体系，有效实现威胁对抗大闭环，对安天人来说是一个艰难的过程，也是必须完成的突破。这也是我们把本届冬训营营语定为“寒夜远征”的原因，“寒夜”是严峻的安全威胁挑战，“远征”是我们达成目标的信念与行动。智者安天下，安天将与客户携手，共同创造网络安全防御的未来。

微信扫描二维码阅读原文