安天智甲有效阻断 AIDS NT 2020 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 AIDS NT 2020 的勒索软件。该勒索软件最早发现于 2020 年 9 月，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。该勒索软件程序执行后，未发现有加密文件的行为，程序通过阻止用户的正常访问操作实现勒索。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 AIDS NT 2020 勒索软件的勒索行为。

AIDS NT 2020 勒索软件样本运行后，删除桌面上的所有文件；并在 windows 目录中创建名为“AIDS_NT_Instructions.txt”的勒索信；拷贝勒索信到桌面文件夹中，该勒索信内容包含勒索说明、以字符串“RYE94xWPXwQZSlIqItLDUA”为社交软件 Telegram 账号的联系方式；样本通过禁止用户访问文件驱动器、禁用相关计算机管理工具（如任务管理器、注册表和控制面板等）和劫持可执行程序及系统功能的运行并指向记事本程序等手段，阻碍用户在系统上的所有正常访问操作实现勒索；最后为关闭正在运行的程序和更新上述设置，系统将在一分钟后重启，重启后自动打开勒索信。

▲AIDS NT 2020 勒索信

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，安天追影产品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、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、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、反病毒引擎鉴定器、关联分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	AIDS NT 2020.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	925 KB
MD5	14EEFB80A0813ABBF8710387A5383F08
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Wacatac
判定依据	BD 静态分析

◆ 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

◆危险行为

行为描述	危险等级
查询系统硬盘大小	★★★
延时	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取系统信息（处理器版本、处理器类型等）	★
创建窗口	★
打开自身进程文件	★
读取自身	★★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天官方微博　安天官方微信
主办：安天　2020 年 9 月 14 日 (总第 247 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

2020 年国家网络安全宣传周开幕 安天分享产品技术能力和实战经验

9 月 14 日 -20 日，2020 年国家网络安全宣传周于今日在全国范围内统一举行。开闭幕式、网络安全高峰论坛等重要活动在河南郑州举行。本届网安周由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等十部门联合举办，主题为“网络安全为人民，网络安全靠人民”。

本届网安周结合疫情防控实际需要，全国各省市地区网安周活动均以线上为主，充分发挥网络传播优势。其中，郑州主会场设置“2020 年国家网络安全宣传周线上平台”（http://www.gjwlaqxcz.cn），整合数字化展会，全民网络安全知识竞赛、网络安全特别节目、网络安全线上讲堂等多种线上活动，让人们充分参与其中，提升民众网络安全意识。

安天积极参与本届网安周各项活动，亮相郑州主会场，黑龙江、山东、重庆、内蒙等地分会场数字化展会，传播网络安全知识，展示安天体系化产品能力

推介产品服务 达成客户有效防护

在本届网络安全宣传周上，安天展示了态势感知平台、资产安全运维平台以及智甲终端防御系统、探海威胁检测系统、追影威胁分析系统、捕风蜜罐系统、拓痕工具箱等基础安全产品和应用案例。安天资产安全运维平台作为本次展示的重点，在不久前中国网络安全产业联盟公布的“2020 年优秀网络安全解决方案和网络安全创新产品”评选活动中，凭借自身优秀的设计理念、成熟的产品能力和技术创新能力获得年度网络安全创新产品奖。

安天资产安全运维平台是一个综合管理平台，面向规模化的信息资产管理场景，提供安全运维门户、资产管理、配置管理、漏洞与补丁管理、日志与告警管理、日常安全管理等功能，协助管理人员摸清资产底数，建立统一高效的补丁更新体系，形成能与资产与业务融合的整体安全策略调整机制，实现集约化、自动化、精细化的资产安全运维管理。

做客网安进行时 回应行业焦点问题

作为中国网络安全产业联盟理事长，安天创始人、董事长肖新光受邀做客网安周特别栏目“网安进行时”。

在节目中他表示，随着我国信息化水平不断提高，人们的生活高度依赖于网络和信息化系统，高价值信息资产成为高级网空威胁行为体所关注和攻击的目标。在复杂严峻的网络安全威胁形式下，防守方要在攻防博弈中掌握主动权，把网络安全防护工作引导贯彻到信息化建设的全过程中，必要的网络安全防御能力，建立动态综合的网络安全防御体系，达成有效防护，减少攻击所带来的损失。

在面对新冠疫情这种重大社会风险事件时，人们对互联网基础设施的依赖度加大，致重要的信息资产暴露面增加，防御难度加大。在该背景下，要提升我国关键信息基础设施和政企网络安全防御能力，应完善重大社会风险协同研判指挥机制、建立“网信民兵”体系，应对高级网空威胁行为。

提升产品有效防护能力 助力网络安全人才培养

在本届网安周上，安天创始人、董事长肖新光将在网络安全产业创新发展主题论坛上发表题为《以威胁框架为参照系的产品能力演进》的主旨演讲。

他表示，当前网络安全正在经历能力导向建设模式的变革。网络安全规划方法不断系统化和完善；大量机构都在建设态势感知管理平台等顶层能力；新技术、新理念、新产品，也不断涌现。在这种背景下，安全产品对抗威胁的能力的有效性提升迫在眉睫。

威胁框架是认知威胁的重要方法，也是安全厂商提高客户安全防御能力、达成客户安全价值的有效途径。安天对标威胁框架改善产品能力，全线产品的告警和知识标签输出已经靠拢到威胁框架体系，并不断通过威胁框架为参照系，完善安全引擎、产品能力和分析支撑工作。在今年 6 月，为了让客户更深入了解安天产品能力，安天正式公布了各主线产品对应威胁框架的检测、防御相关能力映射图谱，并每年发布更新。

此外，安天资深副总裁潘柱廷将在网络空间安全学科建设与人才培养主题论坛上发表题为《从人才培养到人才检验 - 平行仿真的真需求》的主旨演讲，围绕网络安全人才培养和平行仿真领域话题展开。演讲完整内容将在之后发布，敬请期待。

作为引领威胁检测与防御能力发展的网络安全国家队，安天自 2014 年起积极参加每届国家网络安全宣传周，宣传网络安全知识，分享技术积累和实战经验，为“共建网络安全，共享网络文明”作贡献。

扫码进入
2020 网安周官网

扫码进入
CCIA 优秀创新成果展

每周安全事件

类 型	内 容
中文标题	美国 SeaChange 公司遭到 REvil 勒索软件攻击
英文标题	Leading US video delivery provider confirms ransomware attack
作者及单位	Sergiu Gatlan
内容概述	总部位于美国的领先视频交付软件解决方案供应商 SeaChange International 证实，该公司在 2020 年第一季度遭遇勒索软件攻击，导致业务中断。当时 REvil（又名 Sodinokibi）勒索软件团伙承认了 SeaChange 公司的攻击事件，他们为 SeaChange 创建了一个新的受害者页面，该页面用于发布 REvil 操控者所说的攻击期间的文档快照。
链接地址	https://www.bleepingcomputer.com/news/security/leading-us-video-delivery-provider-confirms-ransomware-attack/

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	威胁等级	简要描述
活跃漏洞	Microsoft Office 安全漏洞（CVE-2020-1563）	高	当 Microsoft Office 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用该漏洞的攻击者会在当前用户的上下文中运行任意代码。如果当前用户使用管理员用户权限登录，那么攻击者就可以控制受影响的系统。
	Windows 状态存储库服务安全漏洞（CVE-2020-1512）	高	当 Windows 状态存储库服务不正确地处理内存中的对象时，存在信息披露漏洞。成功利用此漏洞的攻击者可以获取信息，从而进一步入侵用户系统。攻击者可以通过在受害者系统上运行经特殊设计的应用程序来利用此漏洞。
	Microsoft Word 安全漏洞（CVE-2020-1583）	高	Microsoft Word 无法正确显示内存内容时，存在信息泄漏漏洞。利用此漏洞的攻击者可以使用这些信息来入侵用户的计算机或数据。为了利用该漏洞，攻击者可能制作一个特别的文档文件，然后诱使用户将其打开。
较为活跃样本家族	Trojan[Banker]/Win32.Emotet	中	此威胁是一个具有窃取银行账户行为的木马家族。该家族木马在执行后会在后台对进程进行监控，监视登陆银行页面的进程并记录信息，回传攻击者服务器。
	Trojan[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Worm[Email]/Win32.Runouce	中	此威胁是一种可以复制自身并传播的蠕虫病毒家族。该家族的蠕虫通过预览恶意邮件触发，还能利用局域网进行传播，并导致局域网的所有机器都成为恶意邮件的“发送基地”。
	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/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[Banker]/Android.Gustuff	中	此威胁是安卓平台上的一种银行木马家族。该家族木马通过恶意简讯进行传播，存在窃取金融凭证、自动执行交易和进一步感染用户的其他联络人等行为。

将物理安全纳入数据泄露防护

苏·波伦巴 / 文 安天技术公益翻译组 / 译

如果企业在公有云上处理大部分业务数据和工作负载，就容易忽视本地服务器。在办公楼空置（远程工作）的情况下，员工可能会认为，本地服务器的物理安全水平与其他设备是一样的。实际上，物理安全有其自身的特性，确保服务器的物理安全可以减少数据泄露发生的可能性。

数据泄露的成本

现在，许多企业开始远程运营，他们对公有云和托管服务的依赖性比以往任何时候都要高。但是，他们仍然需要本地服务器和私有云，特别是那些处于具有严格合规要求的行业的企业。对他们来说，保护数据免遭侵害（包括物理侵害）至关重要，尤其是当数据涉及客户个人身份信息（PII）时。

由 Ponemon Institute 编写，IBM Security 发布的《2020 年数据泄露成本报告》指出，80％的数据泄露事件涉及客户 PII。报告指出，涉及客户 PII 的数据泄露成本最高，每条记录丢失或被盗的平均成本为 150 美元。当客户 PII 受到恶意攻击者或内部人员的侵害时，这些成本会更高，达到每条 175 美元。

改善现场数据服务器的物理安全性可能需要前期投资，但是这种投资是值得的，这从投资回报率（ROI）可以看出。《2020 年数据泄露成本报告》指出，10％的恶意数据泄露是由物理安全漏洞所致，造成的平均损失为 436 万美元。

将物理和数字安全结合起来

如果企业认为数据泄露都是由恶意软件感染、凭证被盗或笔记本电脑丢失导致的，那可就错了。而且，在合规官和数据泄露法规看来，数据泄露是如何发生的并不重要。如果数据被未经授权的人员以任何方式破坏，就说明数据已经被泄露了。

数据服务器应配备网络安全系统和工具，以防止数据泄露。但是，很多员工并不重视物理服务器的安全性。攻击者可以通过多种方式破坏物理服务器，从而窃取数据。

1. 未经授权地进入服务器机房

攻击者可能会设法进入服务器机房，并通过设置远程访问权限或将恶意软件直接下载到服务器上来控制企业的网络。此外，员工过失也会导致此类数据泄露——例如，有访问权限的员工邀请未经授权的员工进入服务器机房或访问特定服务器。

2. 硬盘窃取或损坏

攻击者可能会窃取或损坏服务器硬盘，导致数据丢失。备份解决方案也可能会遭到攻击。如果企业没有适当地保护服务器（将其锁起来），则攻击者可能会窃取服务器本身。

3. 在服务器机房中安装流氓设备以创建据点

攻击者可能会设计和安装流氓设备，从服务器窃取 PII 和其他敏感信息。

防止物理数据泄露的建议

企业可以参考以下建议，提高数据服务器的物理安全性。

●如果可以，企业应部署生物识别技术。在服务器机房入口处使用生物特征扫描仪，可以减少未经授权进入的情况。

●为入口系统部署保护措施。一次只能允许一个人通过的旋转门或人孔门系统能够防止未经授权的人员尾随进入。

●将每台服务器作为独立单元处理。设置不同的口令、上锁、多因子身份鉴别和最低访问权限等措施，可能无法完全保护服务器免受物理破坏。但是，这些措施会使攻击者更难劫持企业的基础设施。

●根据服务器上数据的敏感性，企业可以在服务器机房中安排保安或安装安全摄像头进行监控。此外，企业应部署结合了多种访问控制（包括证件扫描、密钥代码和生物特征识别等身份识别技术）的锁定系统，将其作为最低的物理安全标准。

●物理安全也意味着防止自然灾害的影响。黑客并不是破坏企业数据的唯一威胁。停电、火灾、洪水和其他恶劣天气情况都可能影响本地数据中心。企业需建立各种系统，主动管理各类自然灾害。

即使公司将大部分数据迁移到公有云，他们也需要本地服务器。只要这些服务器存储着公司数据，就有数据泄露的风险。企业需要确保其物理安全性，以保护其中的数据。

原文名称	Data Breach Protection Must Include Physical Security
作者简介	苏 · 波伦巴（Sue Poremba）。苏 · 波伦巴是一位作家，擅长网络安全和技术领域。
原文信息	2020 年 9 月 8 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/articles/data-breach-protection-physical-security/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。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。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。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，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。