安天智甲有效防护 Badbeeteam 勒索软件

勒索软件名：Badbeeteam 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.CRPTD
支付与金额：通过邮箱与攻击者联系
免费解密工具：暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Badbeeteam 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。该勒索软件运行后，将在短时间内完成对计算机文件的加密操作。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 Badbeeteam 勒索软件的加密行为。

Badbeeteam 勒索软件样本运行后，首先，该勒索软件会在 %appdata%\microsoft\visio 目录释放 4 个文件，分别是名为“Recover files.hta”的勒索信、卷影删除脚本、勒索信脚本和 UserID 文件，同时将自身和勒索信脚本路径加

▲Badbeeteam 勒索信

入到注册表启动项中，实现开机自启动；其次，加密计算机上的所有文件，在被加密文件的后缀名后追加以“.CRPTD”命名的后缀，将勒索信拷贝至计算机上的所有文件夹下，执行卷影删除脚本，具体有删除卷影和关闭相关数据库服务等操作；最后，执行勒索行脚本，弹出勒索信窗口，具体内容有勒索说明、联系邮箱和 UserID 等。

Badbeeteam 勒索软件采用“AES+RSA”加密算法，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。

感染式恶意代码

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述感染式恶意代码进行有效检测，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、关联分析鉴定器、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、来源信息鉴定器、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、关联分析鉴定器、反病毒引擎鉴定器动态行为鉴定器将文件判定为感染式恶意代码。

◆ 概要信息

文件名	Badbeeteam.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.29 MB
MD5	F4C92C5896D92368DAB37F277F74220A
病毒类型	感染式恶意代码
恶意判定 / 病毒名称	Virus/Script.AGeneric
判定依据	反病毒引擎

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	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
查询系统硬盘大小	★★★
感染文件	★★★★
延时	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统信息（处理器版 本、处理器类型等	★
.....	.....

◆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 10 月 19 日 (总第 250 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天开放资料平台上线，安天周观察新航道

致各位尊敬的《安天周观察》读者：

《安天周观察》至今已至今累计发放 250 期，每月向客户、专家、主管部门报送近千份纸质版《安天周观察》，周观察内容受到客户、领导、专家、业内友人们的广泛认可。

随着移动互联网的发展，无纸化阅读成为人们的主流阅读方式，手机阅读成为人们获取知识、资讯的第一选择。因此，在广泛听取专家领导和各位读者的建议后，我们决定改变之前邮寄纸质版的方式，而以电子版形式继续向各位分享技术和资讯。

同时，为了使读者更为方便、快捷的查阅《安天周观察》等内容，我们搭建了开放资料平台，面向客户、主管部门、技术人员免费分享所有技术报告和安全资讯合集。微信扫描下方二维码即可进入平台。

扫码进入“安天开放资料平台”

助力石油石化
安天亮相中国智能油气管道与智慧管网技术交流大会

10 月 14 日 -17 日，第二届“中国智能化油气管道与智慧管网技术交流大会暨山区油气管道安全与智慧运行技术交流会”在成都成功召开。来自国家工信部、国资委、国家能源局相关领导，中国工程院、中国科学院院士，中国石油、中国石化、中国海油、国家管网、中国航油等单位主管领导和专家，大专院校和研究机构的知名专家和学者们 800 余人出席。

大会以“推进智能管道 / 智慧管网建设，深化山区管道关键技术，助力管道业务高质量发展”为主题，旨在为加快推进“互联网 +”与油气储运领域的深度融合，推动智能化技术在管道全产业链应用，引领管道建设与运行向自动化、数字化、可视化和智能化发展，提升管道安全水平和运营效益，为油气管道业务高质量发展提供强有力技术支撑。

安天作为引领威胁检测与防御能力发展的网络安全国家队，积极参与本次会议及展览。结合油气储运建设行业的网络安全需求和特点，安天向与会专家、领导展示了智甲终端防御系统、探海威胁检测系统、追影威胁分析系统、捕风蜜罐系统等安全产品，与安天态势感知解决方案。

安天态势感知解决方案以“敌已在内、敌将在内”的敌情想定为设计前提，展开协同响应与处置的积极防御，高效地实现威胁与脆弱性检测识别、安全事件理解分析、攻击与影响预测、协同联动处置、情报与知识生产，实现安全态势的全面感知与安全业务的融合贯通，对日趋复杂的网络攻击进行更为精准地发现与打击，从而保障响应行动的及时性和有效性，支撑协同联动的实战化运行，协助用户筑起可对抗高级威胁的网络安全防线。

安天多年来深耕能源领域网络安全发展建设，始终站在威胁对抗的第一线，协助客户构建动态综合的网络安全防御体系，达成有效安全价值，赋能客户筑起可对抗高级威胁的网络安全防线。

每周安全事件

类 型	内 容
中文标题	Silent Librarian 针对学校进行网络钓鱼攻击
英文标题	Silent Librarian APT right on schedule for 20/21 academic year
作者及单位	Threat Intelligence Team
内容概述	9 月中旬，Malwarebytes 研究人员发现 Silent Librarian（TA407、COBALT DICKENS）组织积极针对学校进行网络钓鱼攻击。Silent Librarian 通过建立大量的网络钓鱼站点进行攻击，目标并不局限于特定的国家。攻击者使用 Cloudflare 作为大多数钓鱼域名，以隐藏真正的域来源，但研究人员通过分析能够确定其位于伊朗的一些基础设施。
链接地址	https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-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	Windows Media 安全漏洞（CVE-2020-1508）	高	Windows Media 中存在安全漏洞。该漏洞源于 Windows Media 音频解码器不正确地处理对象，攻击者可利用该漏洞获取用户信息。
	Microsoft Windows Jet 数据库安全漏洞（CVE-2020-1074）	高	Windows Jet 数据库存在安全漏洞，该漏洞源于不正确地披露其内存中的内容。攻击者可利用该漏洞执行任意代码。
	Windows GDI 安全漏洞（CVE-2020-1285）	高	Windows GDI 中存在安全漏洞。攻击者可借助该漏洞控制受影响的系统，可以安装程序；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.Yakes	中	此威胁是一种木马类程序。该家族可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	Trojan/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan[Packed]/Win32.Upantix	中	此威胁是一种可以窃取密码信息的木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan/Win32.Blamon	中	此威胁是一种可以释放比特币挖矿机的木马家族。该家族样本运行后释放恶意代码到本机 并运行，连接网络下载比特币挖矿机，占用系统资源，影响用户使用。
	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[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。

如何避免身份管理项目中的常见错误

约翰·米尔本 / 文　安天技术公益翻译组 / 译

20 多年来，在身份和访问管理（IAM）领域，我经常看到这样一个问题：为了实施更强大的身份治理和管理（IGA）计划，企业启动了相关项目；但是，即使有良好的开端，整个项目也会在 6 到 12 个月内分崩离析。

IGA 计划所谓何用

审计和合规团队试图减轻监管风险，但是此类风险却持续增长。时间和资金的浪费，使审计和合规团队感到沮丧，甚至感到焦虑。这导致各方相互指责，出现争论和不和问题。

经过调整的、高效的 IGA 计划值得企业进行投资。IGA 计划有助于确保企业的数据安全，协助企业完成审计并大幅提高运营敏捷性。

IGA 项目中的三个常见错误

鉴于各公司情况不同，他们出现问题的地方也各不相同。但是，这些问题大同小异，特别是下述三个常见错误。

1. 低估成本

IGA 项目不仅涉及 IT 部门，还涉及其他多个部门。企业不应仅将 IGA 视为购买和安装软件——这个错误是可以避免的。IGA 项目要想正常运作，不仅需要内部资源，还需要外部咨询服务。如果项目人员不了解 IGA 进程的相互关联性，就会低估应用集成成本。例如：IGA 解决方案通常与人力资源（HR）管理系统关联；培训费用可能超出项目人员的预期；寻找具备 IGA 技能的人员花费的时间和资金也往往超出预期。

2. 不考虑用户体验（UX）

IGA 最终用户希望能够轻松使用 IGA 系统。如果无法实现这一点， 整个项目就会陷入危险之中。用户希望能够使用该系统完成工作，他们通常没有时间或兴趣来学习新的系统和词汇。如果使用该解决方案还要额外付出精力进行学习，那么用户就不会使用。他们会致电服务台或与同事，表示他们无法完成 IGA 任务。这种不配合会破坏 IGA 项目

3. 无法获得或维持高管支持

IGA 项目具有挑战性，需要跨部门的协作。强大的高管支持对于成功克服潜在摩擦至关重要。根据我的经验，一旦高管支持人不再参加状态会议，就表示项目遇到麻烦了。这通常不是高管的错——他们太忙了，而且未被告知其对于确保 IGA 投资取得良好成果的重要性。

如何避免上述问题

这些问题不应成为IGA项目的绊脚石。企业应意识到这些问题并在项目计划阶段予以解决。准确地进行预算，考虑用户体验，向高管支持人明确说明期望，是 IGA 项目成功的基础。

在 IGA 项目实施过程中，有一种新方法可以发挥巨大作用。该方法就是将 IGA 工具集与现有的应用平台（员工使用该平台处理 IT 相关工作）集成。大多数企业都有这样的平台，ServiceNow 就是一个很好的例子。

在现有平台上构建 IGA 项目，有以下优势：

- 能够最大程度地利用现有平台
- 与购买 IGA 解决方案相比，该方法的成本更低；企业可以将节省的资金用于其 IGA 构建和管理。
- 不需要新的技能，避免了独立 IGA 解决方案带来的成本高昂的人才招募 / 培训 / 保留工作。
- 如果 IGA 系统在现有平台上运行，对其进行更改也会更经济。

员工已经在使用平台接口，因此启动与现有进程无缝集成的 IGA 项目不会出现多少培训或用户体验问题。员工知道请求和批准身份管理服务的接口和工作流程。他们不必保存新的 URL 或学习新的工作方式，这能够加快整体接受度。

应用平台日益成为数字转型（DX）项目的主要工具之一。考虑到数字转型愿景中 IT 敏捷性和平稳 IT 运营的重要性，这是有道理的。将 IGA 与数字转型相关联，可以更轻松地吸引高管加入 IGA 项目。

支持数字转型项目的高管决定着项目的发展。他们知道数字转型项目前景光明，而且可能会带来强劲的投资回报。将 IGA 添加到数字转型项目中，身份管理项目就不会被忽视。

在启动 IGA 项目时，企业应避免常见错误，这需要付出一定的精力，但是由此带来的回报会很丰厚。如果企业希望更新或改进当前的 IGA 项目，可以考虑利用现有的平台来获得最成功的结果。

原文名称	How to avoid the most common mistakes of an identity governance program
作者简介	约翰 · 米尔本（John Milburn）。约翰 · 米尔本是 Clear Skye 首席执行官。
原文信息	2020 年 10 月 9 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/10/09/avoid-common-mistakes-iga-program/
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。