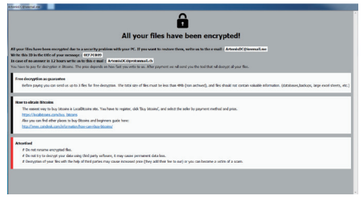
安天智甲有效防护 Kobos 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Kobos 的勒索软件。该勒索软件最早于 2020 年 12 月被发现，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。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 Kobos 勒索软件的加密行为。

Kobos 勒索软件样本运行后，创建多个线程，在短时间内完成对计算机上相关文件的加密，并为被加密文件添加包含 8 个字节随机字符、邮箱及“kobos”字样的文件名后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“## HOW TO RECOVER ##.hta”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱以及获取比特币的途径。为了诱导受害者尽快缴纳赎金，勒索信中强调了赎金金额将取决于受害者通过电子邮件联系攻击者的时间。



▲Kobos 勒索信

Kobos 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，下为其自动生成的分析报告：

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、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、 动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	kobos.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	307 KB
MD5	99D3CC737B0AE28A9993186213D2A6F7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Bulz
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
删除全盘所有卷影副本	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
检测自身是否被调试	★★
镜像劫持	★★
检索系统内存信息	★
获取计算机名	★
读取自身	★
访问文件尾部	★
壳行为填充导入表	★★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2020 年 12 月 28 日 (总第 260 期) 试行 本期 4 版 扫描上方二维码查询安天所有对外开放资料

安天参与承办 2020 中国等保大会召开

12 月 20 日，“2020 中国网络安全等级保护和关键信息基础设施保护大会”（以下简称大会）在南宁隆重召开。本次大会由公安部网络安全保卫局、国家密码管理局商密办、中国科学院办公厅指导，公安部第一研究所主办，安天、深信服、启明星辰、绿盟等 10 家网络安全企业联合承办，旨在推动促进网络安全等级保护和关键信息基础设施安全保护工作，加强业务交流和经验分享，健全国家网络安全综合防控体系。

公安部网络安全保卫局一级巡视员、副局长、总工程师郭启全，广西壮族自治区公安厅党委委员、一级巡视员李跃，国内政商学研各界领导、专家、学者、企业家、从业人员，共同围绕新基建网络安全、等级保护技术、关键信息基础设施保护策略和机制、新技术新应用安全风险和管控、网络安全产品等热点领域，交流分享最新研究成果、技术路线、解决方案和最佳实践。

大会现场

安天高级副总裁王小丰在“新技术新应用安全分论坛”上带来了《威胁情报和检测引擎结合，有效提升安全防护能力》的主题演讲，分享了威胁情报的应用现状和挑战、安天的威胁情报和检测引擎结合的实践，以及相关应用效果等，获得参会领导及嘉宾的关注和肯定。

安天高级副总裁王小丰发表主题演讲

2020 年 9 月，公安部制定出台《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，明确以保护关键信息基础设施、重要网络和数据安全为重点，切实加强保卫、保护和保障；并提出全面加强网络安全防范管理、监测预警、应急处置、侦查打击等各项措施，及时监测、处置网络安全风险和威胁。

在等保 2.0 中，对云、移动终端、无线等场景的安全要求进行了强化，广泛强化了对恶意代码的安全威胁的检测处置能力的部署，对安全策略、补丁升级等做出了集中管控的要求。这些与安天的场景布局和产品能力沉淀高度一致。

王小丰副总裁表示，安天始终致力于有效应对安全威胁，全面提升客户的网络安全防御能力。安天对等保 2.0 进行了充分对标分析研究，可以更好地帮助客户构建全面满足等保要求的网络安全防御体系。

伴随着 APT 攻击、以及定向勒索 + 曝光用户数据相组合等新兴威胁，客户数据资产面临巨大风险，用户需要有效的威胁检测、防御、捕获、分析、处置等基础能力。安天积极对标威胁框架提升产品能力，2019 年 6 月 30 日起，安天引擎和铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信等全线产品已将事件类型和标签体系切换到 ATT&CK 威胁框架，形成能有效发现、识别、阻断和呈现对手杀伤链的安全能力支点。安天发挥自主研发的威胁检测引擎的基础能力优势，持续提高威胁情报生产分发能力，赋能全环节安全运营：针对重点威胁，利用威胁动静态自动化分析与人工分析结合、生产更深度的情报信息；针对非重点威胁，利用全量格式解析，支撑威胁分析和潜在威胁发现；针对高级威胁行为体，融合整编更具价值的信息。

扫描上方二维码阅读原文

研究人员发现 Emotet 僵尸网络的新恶意文档活动

在沉寂了近两个月后，Emotet 僵尸网络带着更新的有效载荷再次出现。新的 Emotet 恶意文档包含了一个明显的变化，可能是为了防止受害者注意到他们刚被感染。该文档仍然包含用于安装 Emotet 的恶意宏代码，并且还是声称是一个“受保护”的文档，需要用户启用宏才能打开它。旧版本在启用宏后不会给出任何可见的响应，新版本会创建一个对话框，显示“Word 在试图打开文件时出错”。如果用户运行恶意宏就会安装 Emotet 恶意软件，它本身也有一些更新。该恶意软件以前是带有“.exe”文件名的独立可执行文件，但现在是使用内置 Windows 程序 rundll32.exe 初始化的 DLL 文件。Emotet 的命令和控制（C2）通信也已更改为使用二进制数据而不是纯文本，这可能会使在网络级别更难检测。最后，作者修改了二进制文件，以阻止 C2 细节和其他 IOC 的提取。

（原文链接：https://cofense.com/emotet-is-back-for-the-holidays-with-updated-tactics/）

每周安全事件

类 型	内 容
中文标题	SolarWinds 黑客入侵美国财政部官员的电子邮件帐户
英文标题	SolarWinds hackers breached US Treasury officials’ email accounts
作者及单位	Sergiu Gatlan
内容概述	美国参议员罗恩 · 怀登 (Ron Wyden) 表示，数十个美国财政部的电子邮件帐户遭到了 SolarWinds 黑客背后的威胁行为者入侵。据财政部工作人员的说法，该机构从 7 月份开始遭受了严重的违规行为，其严重程度不得而知。微软通知该机构，数十个电子邮件账户被盗。这位参议员还补充说，SolarWinds 黑客还入侵了美国财政部部门办公室的系统。怀登说：“财政部仍然不知道黑客采取的所有行动，或者确切地说窃取了什么信息。”
链接地址	https://www.bleepingcomputer.com/news/security/solarwinds-hackers-breached-us-treasury-officials-email-accounts/

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 PowerPoint 安全漏洞（CVE-2020-17124）	高	由于 Microsoft SharePoint 对用户输入验证不足，攻击者可以输入一些精心构造的数据，造成内存破坏，从而导致远程代码执行。
	Microsoft Windows Hyper-V 安全漏洞（CVE-2020-17095）	高	Windows Hyper-V 无法正确验证来宾操作系统上经身份验证的用户的输入时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。
	Microsoft Edge 安全漏洞（CVE-2020-17131）	高	Microsoft Edge 存在一个安全漏洞，攻击者可利用该漏洞可以远程执行恶意代码。
较为活跃样本家族	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。
	Trojan/Win32.Blamon	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[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	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.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	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。

获取情境信息是缩小攻击面的关键：三个原因

吉迪·科恩 / 文 安天技术公益翻译组 / 译

2020 年，网络安全领域发生了根本性的变化。“禁足令”迫使企业寻求维持连续运营的新方法。这导致的结果是，企业将数字化转型计划从三年期加速为三个月。许多企业未经仔细斟酌就进行了云迁移。这种加速的数字化转型是企业不得已的选择，他们将 IT 和安全团队联合起来以协调旧技术、识别供应链中的风险、缩小不断扩展的攻击面，重新调整计划以支持核心业务目标等。为了重新获得并保持控制力，IT 和安全团队需要围绕一个核心点进行协作：在整个企业中获得完全的可见性。

技术扩张导致风险增加

如果不了解企业基础架构、资产及其漏洞的情境信息，安全问题将会非常复杂，无法进行管理。当今，企业典型的六层技术堆栈包括网络、存储、物理服务器、虚拟化、管理和应用程序层。

Aberdeen Research 的研究指出，目前，企业的技术堆栈可能涉及 50 多家供应商的 300 多种产品，而这些产品则涉及超过 16 亿个版本的技术安装。而在此之前，企业平均使用 75 种安全产品来保护其网络。目前的数字远远超过了这一平均值。

现在，我们想象一下，企业仍然采用旧系统架构，但数千名员工全部转向远程办公并同时使用云服务，会出现什么状况。安全团队几乎要在一夜之间开始实施新的网络配置和安全控制，仓促之下很可能会出现配置错误，引入新的风险。

安全团队需要配置更多的入口和出口点，保护更多的技术，并验证更多的变更。要想平衡有限的人员和不断增长的业务需求，同时解决不断增长的风险，唯一的方法是了解企业环境的情境信息，从而更明智、更有针对性地降低风险。

获取数据并了解相关情境消息

要想了解企业资产的网络风险及其情境信息，需要对企业 IT 和安全堆栈中的整个技术生态系统有一个整体的了解。许多企业正在将新的安全产品引入其堆栈。不幸的是，这些新工具通常孤立地解决单点问题，很少能深入了解攻击面和潜在风险，只会产生有限的影响。

企业应收集、汇总和归纳所有解决方案中的数据，以便了解风险，提高查看各方面问题的能力。这种能力会越来越重要，特别是考虑到网络的不断变化及其边界的消失。要想降低风险，一次或定期的努力将不再奏效。

为了妥善保护如今的数字化企业，首席信息安全官（CISO）开始实施情境感知的变更管理流程，该流程能够平衡 IT 基础架构及其支持的应用程序的每日快速变更需求，并能够持续确保企业安全。

以下是企业实施该流程的主要原因。

1. 企业无法保护看不到的东西

威胁响应与新安全策略和配置的实施缺乏融合，这造成了攻击者可以利用的安全盲点。随着企业边界的不断消失和远程办公的持续存在，安全人员必须重新考虑和计划新的网络防御，并获取相关情境信息，以支持果断、有针对性的行动。

2. 跟上变更的脚步

无论企业需要管理混合型远程员工还是企业范围内的软件实施，“新常态”都比以往需要更大的灵活性和变更。如果安全策略管理团队在不了解漏洞和资产风险的情况下验证新策略并部署新规则，通常会在无意间引入新风险。

为了对安全策略变更进行适当的分析和部署，领先的企业着手开发变更管理实践，以弥合安全团队与网络团队之间的鸿沟。实施情境感知的策略变更，利用网络路径分析和攻击模拟功能，可以在确保企业敏捷性的同时保护其安全。

3. 快速制定明智的决策

如果网络安全策略管理和漏洞管理未互联，企业就会缺乏情境信息。最终，这会导致其安全状况不佳。如果企业依靠不充分的被动安全措施，就会为攻击者提供很多可利用的关键漏洞。

网络罪犯分子和攻击者会迅速利用远程办公这种新常态，这意味着安全团队在制定安全决策时要比以往更快。有了网络及其安全策略的统一视图，企业可以更好地关联不同的系统孤岛。借助可以转化为行动的情境信息，安全专家可以集中精力补救最需要的地方，同时快速验证网络配置变更。

今年的疫情促使各种规模的企业重新评估其安全计划、制定新的策略，以改善其安全状况。企业依赖其安全和 IT 团队进行战略决策和执行。在 2021 年及以后的日子里，在确保企业实现目标方面，他们将发挥关键作用。为了扩大他们的影响力，缩小攻击面并支持持续的数字化需求，安全和 IT 领导者需要开发可见性能力。因此，他们需要获取情境信息。

原文名称	Three reasons why context is key to narrowing your attack surface
作者简介	吉迪 · 科恩（Gidi Cohen）。吉迪 · 科恩是 Skybox Security 的首席执行官。
原文信息	2020 年 12 月 22 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/12/22/narrowing-attack-surface/
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。