安天智甲有效防护 Xorist 勒索软件新变种

近日，安天CERT在梳理网络安全事件时发现一个Xorist勒索软件新变种。该勒索软件隶属于Xorist勒索软件家族，最早于2020年10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Xorist勒索软件新变种的加密行为。

该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，在被加密文件的后缀名后追加以“.ZaLtOn”命名的后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“HOW TO DECRYPT FILES.txt”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱、赎金金额。该勒索软件会将自身拷贝到“C:\Users\用户名\AppData\Local\Temp”路径下并操作注册表添加表项，将其设置为开机自启动。

▲勒索信

该勒索软件采用“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、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、智能学习鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	ZaLtOn.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	4.82 MB
MD5	D8722DC3A9ED1845DD6E880808EC5A19
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Xorist
判定依据	反病毒引擎

◆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
移动启动目录，疑似突破主动防御监控自启动目录	★★★

◆常见行为

行为描述	危险等级
自我复制	★★
修改文件创建时间	★★
Run 自启动	★
创建快捷方式	★
疑似查找浏览器进程	★★
设置自启动项	★★
创建桌面快捷方式	★
文档篡改	★★

◆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07日(总第257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

中国网络安全产业高峰论坛开幕 安天获多项能力认可

11月30日，2020年中国网络安全产业高峰论坛在京举行。论坛以“新基建新网安新产业”为主题，由工业和信息化部及北京市人民政府共同主办，工业和信息化部网络安全产业发展中心、北京市经济和信息化局和北京市海淀区人民政府承办。工业和信息化部党组成员、副部长刘烈宏出席开幕式并致辞。安天积极参与本次活动，并获得多个能力认可奖项。

安天三项目获2020年网络安全技术应用试点示范项目授牌

凭借先进的自主研发实力和领先的产品技术架构能力，安天申报的“电力网络安全监测与指挥平台”、“智信零信任应用安全交付服务平台”、“网络空间威胁情报大数据共享开放平台”三个项目全部入选“2020年网络安全技术应用试点示范名单”，并在论坛开幕式上获得授牌。这是国家级部门对安天产品和技术能力的充分认可，也表明了安天在工业互联网安全、智慧城市安全、威胁情报领域的项目实践具有应用创新性、先进性、实用性及和可推广价值。安天将始终坚持网络安全关键技术突破、网络安全技术应用创新，为加快中国新型信息基础设施建设、网络安全公共服务发展贡献力量。

安天被授予“2020年网络安全威胁认定先进单位”称号

安天凭借在威胁报送与认定工作中的突出贡献，被授予“2020年网络安全威胁认定先进单位”称号。安天在与威胁对抗20年的发展过程中构建了先发预警和全面应急响应的能力。并针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如APT组织）及其攻击行动，进行持续监测和深度解析。

2019年安天即入选首批“工业和信息化部网络安全威胁信息共享平台合作单位”，基于安天二十年的历史数据积累，利用安天海量流量侧威胁感知能力和自动化样本采集分析系统，可形成高质量的威胁情报分析和追踪溯源能力；通过安天全量威胁情报系统，可以快速查询可疑IP、可疑域名、可疑URL、可疑邮箱，以及可疑的文件HASH等；利用灵活的检索功能可进行情报的检索与共享，持续为网络安全威胁信息共享平台认定威胁。

安天探海荣获“先进网络安全产品”

在网络安全产业深度对话分论坛上，嵌入安天下一代威胁检测引擎的“探海威胁检测系统”入选“先进网络安全技术能力产品”。

探海威胁检测系统是安天自主研发的网络威胁监测设备，以网络流量为检测分析对象，实现对网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动、病毒扩散传播、木马远程控制等网络行为的检测和告警，能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁。探海可与安天威胁情报服务结合，对多个APT攻击组织的载荷工具和C2基础设施实现带有精确组织指向的告警。探海威胁检测系统可以为政府、军队、能源、金融、交通等行业客户持续提供监测能力，支撑用户的重大活动安全保障、高级威胁监测和安全事件响应。

安天资深副总裁方华受聘首批网络安全创新创业导师

安天资深副总裁、合伙人方华领取聘书（左一）

本次论坛开幕式启动了首届“创客中国”

（下转第二版）

（上接第一版）
网络安全中小企业创新创业大赛，工业和信息化部网络安全产业发展中心公布了首批网络安全创新创业导师。安天资深副总裁方华受聘成为首批网络安全创新创业导师。活动旨在集聚网络安全领域创新创业资源，发挥创新创业导师在推动企业成长、产业发展方面的教育引导和指导帮扶作用。

安天在 20 年的发展历程中，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。通过 20 年自主研发积累，安天形成了威胁检测引擎、移动场景安全、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势。构筑了由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，为客户构建资产安全运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置、零信任接入等安全基石。安天通过为客户建设态势感知平台体系，形成网络安全运行的神经中枢，提升客户统一安全运维水平，通过大规模感知体系、大规模支撑平台，以及快捷精准的威胁情报持续赋能客户。

在我国发展新基建的过程中，需要网络安全同步规划、同步建设、同步运维的一套方法体系和相应的预算保障，也需要通过规划指引全面提升防御能力，通过预算投入支撑网络安全领域的能力建设，才能满足新基建的防御能力需求，保障承载中国数字经济的基础建设。

安天将不忘初心，始终坚持网络安全关键核心技术突破、网络安全技术应用创新，为加快中国新型信息基础设施建设发展贡献更多力量。

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	Drupal 远程代码执行漏洞（CVE-2020-13671）	高	由于 Drupal core 未能正确地处理上传文件中的某些文件名，攻击者可利用漏洞通过上传恶意文件，在某些特定的配置下可能会被当作 php 解析，从而导致远程代码执行。
	Linux kernel 存在安全漏洞（CVE-2020-25704）	高	Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Linux kernel 存在安全漏洞，攻击者可利用该漏洞可以通过 perf_event_parse_addr_filter() 来创建内存泄漏，从而触发拒绝服务。
	Microsoft Excel 远程代码执行漏洞（CVE-2020-17064）	高	由于 Microsoft Excel 在分析经特殊设计的 Office 文件时没有正确处理内存对象，导致 Excel 中存在一个远程代码执行漏洞。此漏洞可能会允许攻击者执行任意代码，从而损坏系统内存。
较为活跃样本家族	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	Trojan[Backdoor]/Win32.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	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/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	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。

如何减轻采用云服务的企业的网络安全风险

胡安·帕勃罗·佩雷斯·埃切戈延 / 文 安天技术公益翻译组 / 译

新冠疫情期间，云迁移和“软件即服务”（SaaS）的应用激增。最近的一项调查显示，疫情使 40％的企业加速了云迁移。企业依靠这些平台和工具的灵活性来提高生产力，无需考虑员工在哪里办公。

互联环境

企业还经常将这些应用连接到关键业务流程，以传输有价值的客户数据、个人身份信息（PII）、财务和其他敏感信息，帮助流程顺利运行。但是，随着越来越多的业务流程从本地扩展到云端，公司开始丧失对其互联应用生态系统风险的可见性。

问题在于，在互联环境中，一个配置错误的系统或一个安全漏洞就有可能会使整个企业面临风险。此外，IT、网络安全、开发和审计团队难以掌握哪些应用和服务支持关键业务流程，这些应用和服务支如何相互连接，以及其更改如何会影响合规性、安全性和可用性。

随着远程办公成为长期性的现实问题，企业开始了“随处运营”。现在，企业是时候考虑以下三个关键问题了，以了解其面临的风险并减轻这些风险。

错误配置带来的风险

企业的数字转型，加之对云服务和“应用程序接口”（API）使用的稳步增长，使得集成和连接来自不同供应商的两个或多个系统越来越容易。但是，无论企业想将 Oracle 与 SuccessFactors 连接，还是将 SAP 与 Salesforce 连接，API 都会带来巨大的风险。

这是因为，许多业务应用反映了基于复杂底层技术构建的工作流和流程。虽说这种集成很容易，但是集成之后，企业面临的是两个高度可配置的、相互融合的应用。自定义这些应用的能力可能会引入各种漏洞，这些漏洞会影响集成、身份鉴别、审计、加密、用户授权等。

为了识别这些风险，企业首先需要对底层技术有更深入的了解。其次是创建一个包含云和本地资产的资产地图，以了解哪些应用相互连接及其正在传输什么数据。

最后，根据安全和合规性法规来分析每个应用及其支持的数据，以更好地了解其安全和合规性方面的差距。例如，根据《通用数据保护条例》（GDPR）分析个人数据，根据《萨班斯法案》（SOX）分析财务信息，根据 PCI 法规分析信用卡数据，以获得某种程度的控制力。

归根结底，一些看似微小的不合规可能会危及整个应用和数据（无论部署在哪，都要由客户保护）的完整性，因此企业必须控制其配置。

用户权限的控制

授权和访问控制是企业风险管理和内部控制的基本组成部分。了解“谁”有“哪些”权限以及“职责分离”（SoD）至关重要，可确保关键职能分散在一个以上的人员或部门中，以减轻欺诈和犯错的风险。

但是，随着企业将应用从本地环境迁移到云环境，以及企业的 IT 部门管不到 SaaS 应用，想要精确了解员工权限越来越难了。此外，攻击者经常假冒企业员工（在云中更为普遍），因此企业应严格控制所有业务应用中的用户权限。从内部角度来看，如果企业不能控制员工权限，员工或攻击者就能轻松地从一个应用移动到另一个应用。

由于某些流程跨多个应用，因此关联用户的能力对于有效控制授权和 SoD 至关重要。为了应对这种复杂性，安全团队还应寻求一种技术，以了解用户在各应用之间的活动，并能在员工未经许可提权时标记异常行为。

采用自动化手段确保持续合规性

Gartner 预计，数据隐私法规的全球监管范围将从 2020 年的 10％跃升至 2023 年的 65％。一些法规会严格监管本地、云和 SaaS 应用，以确保 PII 和财务数据受到保护，这会对运行此类互联网络的企业带来挑战。

传统上，负责确保法规标准的审计团队会进行手动检查以确保合规性。如今，诸如 HR 之类的业务部门经常使用 SaaS 应用（例如 SuccessFactors 和 Workday），这使各个应用相互连接，导致审计团队难以找到真实的来源，因此手动检查变得越来越困难了。手动审计需要进行大量屏幕截图，整理很多 Excel 表格，这需要花费大量时间和资金（数十万美元），但是仅能显示“某个时间点”的结果。

自动化是精简这些繁琐任务的关键。好的解决方案可以智能地分析应用之间的连接，以全面了解合规性错误的根源，以及如何解决这些错误，并推动企业达到“持续合规性”的水平，并以自动化手段控制业务应用，以节省时间和资金，同时遵守不同的合规性法规。

SaaS 和云应用已成为数字化转型的关键因素，它们使员工能够随时随地更有效率地工作。但是，这些应用也会带来严重的合规性和安全风险。如果不能妥善应对这些风险，企业可能会因遭受攻击而登上新闻头条，并遭到巨额罚款。随着公司继续使用 SaaS，他们必须考虑上述三个关键问题，以降低风险，增强安全性并确保持续合规性。

原文名称	How to mitigate risks in an interconnected intelligent enterprise
作者简介	胡安 · 帕勃罗 · 佩雷斯 · 埃切戈延（Juan Pablo Perez-Etchegoyen）。胡安 · 帕勃罗 · 佩雷斯 · 埃切戈延是 Onapsis 的首席技术官。
原文信息	2020 年 11 月 26 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/11/26/how-to-mitigate-risks-interconnected-intelligent-enterprise/
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。