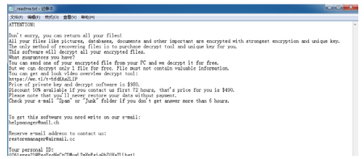
安天智甲有效防护 Jdyi 勒索软件变种

勒索软件名：Jdyi 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.Jdyi
支付与金额：需通过邮箱与勒索者联系
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 Jdyi 的勒索软件变种。该勒索软件隶属于 STOP 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 Jdyi 勒索软件的加密行为。

Jdyi 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“.Jdyi”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“_readme.txt”的勒索信，该勒索信具体内容包含了勒索说明、赎金金额、联系邮箱。为了诱导受害者尽快缴纳赎金，勒索信中强调了在加密后的前 72 小时内付款，则可以节省 50%赎金。



▲Jdyi 勒索信

Jdyi 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。

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、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。

最终依据动态行为鉴定器、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	Jdyi.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	726 KB
MD5	A8D6D7D35598C80FFB2E81A144DEAF22
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.STOP
判定依据	关联分析

◆ 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
访问下载站点	★★★
删除自身	★★★★
修改文件权限	★★★
修改本机 hosts 文件劫持域名	★★★★
禁用任务管理器	★★★
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	★
壳行为填充导入表	★★
自我复制	★★
Run 自启动	★
.....	.....

◆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 11 月 9 日 (总第 253 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天出席 2020 世界计算机大会

11 月 3 日，由湖南省人民政府、工业和信息化部共同主办的 2020 世界计算机大会在湖南省长沙市召开。湖南省委书记杜家毫、工业和信息化部副部长王志军出席大会开幕式并致辞，开幕式由湖南省委副书记、省长许达哲主持。

为期两天的时间里，杨学军、廖湘科、倪光南等十七位中外院士、数十位专家学者及企业家、六百多位产业界精英应邀出席，共探计算产业新动能。4 日上午，2020 世界计算机大会专题论坛“网络安全与可信计算”举行。院士、学者、技术专家等聚焦网络安全关键技术，沟通交流了网络空间安全和可信计算领域的理论热点、关键技术，为网络安全技术创新、产业发展、应用实践凝聚新思路、预判新趋势。

安天科技集团有限公司高级副总裁王小丰在论坛上分享了《采用威胁框架，度量和提升网络安全防护体系》的主题演讲。

他表示，当前，网络安全的攻防态势正发生快速演变，网络攻击的技术手法和作业过程日趋复杂、攻击场景日益多样、攻击危害性剧增，迫切需要更为科学系统的防护体系评估手段，以有效指引和提升网络安全防御建设。

ATT&CK 威胁框架，是业内着眼于网空对抗，实用性、实战价值俱佳的高级威胁分析手段。他介绍和分享了 ATT&CK 威胁框架的安全价值、技术内容及业内部分优秀实践。

王小丰分享了安天在如何有效运用威胁框架，科学度量和系统提升网络安全防护体系的相关实践。并介绍了应用威胁框架评估和提升当前产品能力；应用威胁框架增强针对持续威胁对抗能力；基于威胁框架构建对抗式系统安全评估系统方案的成功案例。

威胁框架既为安全厂商提供了改进点指南，也为我们相关的客户和管理部门提供了如何评价“何为有效的安全产品”的能力参考。安天也将配合监管部门、用户，一同构筑能力型的安全产品，在整个体系化的网络安全解决方案中发挥更大的作用，形成动态综合的防御体系，达成客户有效的安全价值。

VMware 针对 ESXi 的严重漏洞发布了更新修复程序

VMware针对其ESXi虚拟机管理程序产品中的严重远程代码执行漏洞发布了更新修复程序。VMware咨询报告称，在发现10月20日发布的先前补丁无法完全解决该漏洞之后，便可以使用更新的补丁版本，该补丁在2020-11-04年完成了对CVE-2020-3992的不完整修复。该漏洞（CVE-2020-3992）的CVSS评分为9.8（满分10分），非常严重。在通报之前，该漏洞会影响ESXi 6.5、6.7和7.0版本；受影响的产品现已更新，包括VMware Cloud Foundation 3.x和4.x上的ESXi实施。

（原文链接：https://threatpost.com/vmware-updated-fix-critical-esxi-flaw/160944/）

切萨皮克地区 2.3 万份医疗保健数据遭到泄露

切萨皮克地区医疗保健公司Blackbaud从2月7日起经历了一次数据安全事件，该事件可能在5月20日之前间歇性地重复发生。在得知Blackbaud遭遇了数据安全事件后，官员们已经通知了受影响的患者、捐赠者和员工，共计23058人。Blackbaud发现并阻止了一场勒索软件攻击，他们的网络安全团队成功地阻止了网络罪犯的进一步破坏。

（原文链接：https://www.wtkr.com/news/chesapeake-regional-healthcare-alerts-over-23k-patients-after-data-security-incident）

自动化软件销售商 SaltStack 修复了三个错误

SaltStack正式公布了其代码中的三个错误，其中两个很关键，并强烈建议用户优先考虑这次更新。SaltStack提供了基于Python的开源自动化工具，它于10月被VMware收购，该交易完成和扩展其自动化产品并帮助其提供全栈产品。然而，VMware在此过程中发现了三个错误，它们的正式名称是CVE-2020-16846、CVE-2020-17490和CVE-2020-25592。

（原文链接：https://www.theregister.com/2020/11/04/saltstack_security/）

每周安全事件

类 型	内 容
中文标题	研究人员发现了 Windows 中的特权提升漏洞
英文标题	Games in Microsoft Store Can Be Abused for Privilege Escalation on Windows
作者及单位	Eduard Kovacs
内容概述	一名研究人员发现，Windows 系统存在一个特权提升漏洞，可以通过滥用微软商店中的游戏来加以利用。该漏洞被跟踪为 CVE-2020-16877，等级为高，严重影响 Windows 10 和 Windows Server。微软在 2020 年 10 月的 Patch Tuesday 更新中对其进行了修补。
链接地址	https://www.securityweek.com/games-microsoft-store-can-be-abused-privilege-escalation-windows

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 Base3D 远程代码执行漏洞（CVE-2020-17003）	高	Microsoft Base3D 中存在安全漏洞。当 Base3D 呈现引擎不正确地处理内存时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上获得执行权。
	Windows 远程桌面协议 (RDP) 拒绝服务漏洞（CVE-2020-16927）	高	当攻击者使用 RDP 连接到目标系统并发送经特殊设计的请求时，远程桌面协议 (RDP) 中存在拒绝服务漏洞。成功利用此漏洞的攻击者可能会导致目标系统上的 RDP 服务停止响应。
	Windows NAT 远程代码执行漏洞（CVE-2020-16894）	高	当 Windows 网络地址转换 (NAT) 无法正确处理 UDP 流量时，存在远程代码执行漏洞。要利用此漏洞，攻击者可能会在访客操作系统上运行经特殊设计的应用程序。成功利用此漏洞的攻击者可能会在主机操作系统上导致内存损坏。
较为活跃样本家族	Trojan/Win32.Diztakun	中	此威胁是一种使用 .NET 开发的木马类程序。该家族样本运行后会获取系统信息、用户信息和机密数据等，并将这些数据发送到远程服务器。
	Trojan/Win32.Injuke	中	此威胁是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan[Backdoor]/Win32.Finfish	中	该病毒家族是一种可以窃取用户信息的木马类程序。该家族样本运行后修改注册表使其自启动，窃取用户敏感信息，如帐号密码等。
	Trojan/Win32.Sly	中	此威胁是一种可以下载恶意代码的木马类程序。该家族样本运行后连接远程服务器下载恶意代码并运行，有一定威胁。
	Trojan[Downloader]/Win32.Pluto	中	该病毒家族是一种可以下载其他恶意代码的木马家族。该家族样本运行后可以连接网络下载其他恶意代码并安装，可能会窃取用户信息并回传。
	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.Hqwar	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

物联网的零信任访问策略必须细粒度

沙姆斯·麦吉利库迪 / 文 安天技术公益翻译组 / 译

零信任网络架构已经成为主流，但企业可能会发现，物联网（IoT）会给零信任架构带来一些独特的挑战。

在设计零信任访问策略时，用户身份通常是核心变量。当然，还有诸如设备状态、位置、时间和行为等许多其他变量，但是身份是首要考虑因素。

IoT 设备通常没有良好的管理策略，没有用户被赋予其管理职责。因此，企业应采用其他方法来建立访问策略。在 IoT 早期，企业大多采用一种简单的方法——即建立 IoT 虚拟局域网（VLAN），将网络上的 IoT 流量隔离开来。但是，随着物联网不断成熟，某些 IoT 设备可能需要访问敏感数据，VLAN 已不足以保护这些设备。

IoT 访问策略需考虑角色和功能

企业应针对各 IoT 设备的功能和角色，定制细粒度的零信任访问策略。要做到这一点，企业需了解其 IoT 环境。零信任策略引擎不仅要知道 IoT 设备的品牌和型号，还要知道为何安装该设备。

不幸的是，如今大多数企业都没有这样做。2020 年 8 月，企业管理协会（EMA）对 252 位北美和欧洲 IT 专家进行调查，并发布了调查报告《企业零信任网络策略：安全的远程访问和网络分段》。根据该报告，只有 36% 的企业根据角色和功能定制 IoT 访问策略。

28% 的企业创建通用的最低级别访问权限（例如 IoT VLAN），从而降低了零信任访问策略的粒度。这种策略未考虑不同的风险级别。例如，策略引擎不会区分将数据推送到云端和需要从云端提取敏感数据的传感器。这会导致严重的安全风险。

另有 23% 的企业将 IoT 设备视为不受信设备，并大大限制其网络访问。这意味着，其 IoT 设备完全无法访问敏感资产，这限制了企业可以通过 IoT 实现的应用类型。

最后，有 12% 的企业将 IoT 视为完全不受信的，并禁止 IoT 设备连接到企业网络。在这种情况下，他们可能要使用 LoraWAN 或 LTE 之类的移动网络服务连接到云端，从而完全绕开公司网络。

足够的 IoT 可见性，但过于复杂

为何这么多企业没有对 IoT 设备实施细粒度的访问策略？不是因为缺乏可见性。84% 的企业表示，他们对传感器等没有良好管理策略的 IoT 设备具有足够的可见性，可以确定网络访问权限。

问题可能是实施这样的策略过于复杂。大型企业（拥有 10,000 名或更多员工）最不可能确定 IoT 访问权限（23%）。这些大型公司有太多种设备，难以进行分类。相比来说，建立粗略的访问策略会比较容易。

正确实施 IoT 零信任策略：IT 领导层必须予以支持

如果 IT 领导层对零信任策略提供强有力的支持，则企业更容易创建定制的 IoT 访问策略。例如，如果企业拥有正式的零信任网络计划，并专门分配了预算，则很有可能针对 IoT 设备的功能和角色定制访问策略。

相比之下，采用临时零信任方法的企业缺乏专用预算，仅在时间和资源允许的情况下才采用零信任原则，因此更有可能将所有 IoT 设备视为不受信设备，仅允许它们访问低风险网络资产。在这些企业中，生产团队被禁止部署需要访问合规性区域的 IoT 设备。

如何创建定制的 IoT 零信任访问策略

企业需要灵活的零信任访问和分段解决方案，以支持细粒度的 IoT 策略。这些解决方案能够发现 IoT 设备并对其进行分类，监控设备行为，并应用自定义访问策略。

EMA 的研究发现，在创建策略时，IoT 设备的安全状态是最重要的变量。在授予访问权限之前，零信任网络应检查反病毒和反恶意软件的状态。

设备漏洞和风险、设备所有者（例如业务部门）、观察到的网络行为以及操作系统状态等，都是 IoT 零信任访问策略的次重要变量。设备品牌和型号，以及相关的应用程序是最不重要的变量，只有少数企业会使用。

包括设备漏洞和风险评估在内的策略是最佳实践。EMA 的研究发现，结合此变量后，定制的访问策略往往会更加成功。EMA 还发现，网络基础架构团队和信息安全团队之间的协同有助于创建 IoT 访问策略。例如，采用有效工具协同两个团队的企业，更有可能通过这些量身定制的策略获得成功。

EMA 认为，随着时间的推移，针对各 IoT 设备的角色和功能量身定制的细粒度 IoT 访问策略将会越来越重要。我们的研究发现，如今有 75% 的企业网络管理团队支持 IoT 设备连接到企业网络。这个数字将会继续增加；而且 IoT 设备将越来越多样化，并具有不同的访问需求。

原文名称	Zero Trust Access Policies for IoT Must be Granular
作者简介	沙姆斯 · 麦吉利库迪（Shamus McGillicuddy）。沙姆斯 · 麦吉利库迪是企业管理协会（EMA）的网络管理研究副总裁。
原文信息	2020 年 11 月 2 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/network-security/zero-trust-access-policies-iot-must-be-granular
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。