安天发布《Rapid 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Rapid 的勒索软件变种，Rapid 勒索软件最早于 2018 年 1 月被发现，主要通过钓鱼邮件进行传播，邮件附件中包含带有恶意宏代码的 Word 文档，该文档诱使用户启用宏查看文档内容，当用户启用宏后，恶意宏代码将连接 C2 下载并执行 Rapid 勒索软件。

Rapid 勒索软件执行后，加密计算机中的文档文件和可执行文件，将原文件名修改为大写英文字母和数字组合成的十位随机名称，并追加名为“.cryptolocker”的后缀，在桌面和所有含有被加密文件的位置创建名为“userkey.dat”的文件和名为“!DECRYPT_FILES.txt”的勒索信，查看“userkey.dat”文件中的内容为 USER_ID，勒索信内容包含勒索说明和 USER_ID 等。Rapid 勒索软件创建多个线程不断扫描文件，对新创建的文件也进行加密，使用“RSA+AES”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。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口令；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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、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、关联分析鉴定器、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	cd58190be47ca6f416a3fa9c12a65eef70fbe80cfe8a0e098e9ef503b2e62377
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	114 KB
MD5	6961478A6B28B9742142C843DA950D74
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Wacatac
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
删除全盘所有卷影副本	★★★★
在启动时禁用 Windows 错误恢复	★★★★
查询系统硬盘大小	★★★
检测虚拟机	★★★★★
疑似查找游戏进程	★★★★

◆危险行为

行为描述	危险等级
加载运行时 DLL	★
获取驱动器类型	★
枚举进程	★
获取系统版本	★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 12 月 09 日 (总第 211 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

“安天杯”网络安全技能挑战赛

11 月 22 日，“安天杯”网络安全技能挑战赛在哈尔滨工业大学开启。竞赛邀请了东北、华东地区 15 所高校的队伍。经过两天激烈的角逐，Lilac 团队最终斩获第一名。

“安天杯”网络安全技能挑战赛，是由安天和哈尔滨工业大学多年来合办的一项校企联合活动。旨在提升大学生的网络安全意识、网络安全专业技能水平，培养学生的团队合作精神，推动高校信息安全专业建设。比赛题目设置，以防御者视角为主，偏重于取证、分析、加固等安全技能，与其他安全赛事有较大差异。

本届挑战赛题目设置以网络安全防护操作和威胁分析为主，重点锻炼和培养学生对于网络安全威胁的分析、检测、取证相关能力。在赛题设置上，安天联合哈工大网络安全实验室紧密结合近年爆发、曝光的各类安全事件，将协助政企用户准确发现、精确分析和有效处置网络威胁作为赛题场景，本次活动引入“威胁猎杀基础技能”考评（要求参赛选手通过分析网络流量和主机日志等数据，找出攻击者植入主机的木马程序，分析攻击者入侵途径，并提供处置方案）。比赛更加接近网络安全防护和分析的实战要求，较为全面地考

察了参赛选手的综合能力及技术功底。

赛前，大赛组委会组织了一场空中微课，为参赛队伍进行线上指导。组委会向同学们详细讲解多起 APT 攻击事件的事件背景，介绍我国网络安全领域面临的挑战及开展安全防护工作中所要建立的“敌情想定”。同时从爱国主义教育、法制教育和职业道德教育等方面，帮助同学们树立正确的网络安全行业价值导向。网络安全人才培养，需理论学习与技能实训相结合，网络安全技能挑战赛作为一种竞技式的集中实训活动，能够让学生在实战演练中深入理解和使用所学理论知识。参赛同学表示，通过参加本次活动不但提升了网络安全分析相关专业技能，还充分了解了我国在网络空间面对的压力和挑战，感受到了未来自身所肩负的责任与使命。

安天将进一步总结活动中的经验，改进不足，加快推进实战化网络安全演训场的研发。当前，我国网络安全工作中运行、维护、值守、处置等基本操作型技能型人才不足的局面十分明显，安天在发展过程中，也需要大量的研发、分析、产品、服务等相关技术人才。安天网络空间安全学院，将以安全架构、安全开发、安全分析、安全运维工程师培养为重点，培养面向一线的合格网络安全技术人才。

微信扫描二维码阅读原文

伦敦交通管理局锁定了所有 Oyster 和非接触式帐户

伦敦交通管理局已经锁定了所有的 Oyster 旅行卡和非接触式账户，要求用户重新设置密码才能重新登录。早在 8 月份，伦敦交通局 (TfL) 就发现大约有 1200 个 Oyster 账户被“恶意访问”，很可能是在他们使用非 TfL 网站时登录凭证被泄露。现在，作为一项预防措施，伦敦交通管理局要求所有 Oyster 和非接触式账户的持有人重置密码，以降低被盗密码被用来入侵他们的 Oyster 账户的风险。

（原文链接：https://www.zdnet.com/article/got-an-oyster-card-tfl-just-locked-your-account-to-make-you-reset-your-password/）

回购网站泄露了 3.7 万名枪支拥有者的详细信息

政府的枪支回购计划陷入混乱，回购网站的数据泄露影响了逾 3.7 万名枪支持有者的详细联系方式、枪支牌照号码和银行地址。持牌枪支拥有者理事会 (COLFO) 透露了该违规行为，该委员会在下午 12:23 发表声明说，回购网站的用户可以访问有关 70,000 支枪支交接通知的信息。两分钟后，新西兰警方发表声明说，已经知道违规行为，并关闭了现场。COLFO 表示，在警方关闭之前，人们最多可以登录该系统 3 个小时，目前尚不清楚该信息可以公开获取多长时间。

（原文链接：https://www.zdnet.com/article/got-an-oyster-card-tfl-just-locked-your-account-to-make-you-reset-your-password/）

亚马逊计划推出基于面部识别的“观察名单”

据报道，亚马逊计划使用面部识别软件和智能家居安全设备 Ring 来创建一个人工智能的“邻里观察名单”。当一个被认为“可疑”的人被摄像头抓拍时，“观察名单”会自动向手机用户发出“可疑活动提示”。目前还不清楚谁能进入这些社区观察名单，也不清楚如何收集和整理这些名单。

（原文链接：https://threatpost.com/amazon-ring-facial-recognition-watch-list/150681/）

每周安全事件

类 型	内 容
中文标题	研究人员发现微软登录系统中存在安全漏洞
英文标题	A bug in Microsoft’s login system put users at risk of account hijacks
作者及单位	Zack Whittaker
内容概述	以色列网络安全公司 CyberArk 的研究人员发现，微软留下了一个意外的漏洞，如果被利用，这个漏洞可能被用来窃取这些用于访问受害者账户的令牌。该漏洞允许攻击者悄悄窃取账户令牌，这些令牌是在用户登录后由应用程序或网站创建的，以代替用户名和密码。这样可以使用户永久登录到该站点，但也允许用户访问第三方应用程序和网站而无需直接进行操作他们的密码。该安全漏洞已于 10 月下旬报告给微软，并在三周后修复。
链接地址	https://techcrunch.com/2019/12/02/microsoft-login-flaw-account-hijack/

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Locker.by[rog,lck] 2019-12-01	高	该应用程序运行锁定用户界面，加密用户文件，勒索用户付费解密，影响用户手机的正常使用，建议立即卸载。
		Trojan/Android.rekt.a[rog] 2019-12-02	中	该应用程序运行会加密用户 SD 卡下特定格式文件，可能为勒索件的测试程序，建议卸载。
		G-Ware/Android.HiddenAds.jw[exp,rog] 2019-12-03	低	该应用程序安装无图标，后台推送广告，造成用户资费损耗，建议卸载。
	较为活跃样本	Trojan/Android.mobihok.a[prv,rmt,spy]	中	该应用程序是一款远控软件，运行后接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录、键盘记录、文件存储目录、社交应用信息、手机固件信息，私自拍照、录音、录像、截屏、拨打电话、发送短信。并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。
		Tool/Android.bombcall.h[exp]	中	该应用程序是一款电话轰炸程序，可设定向指定的号码进行电话轰炸，需要购买卡密激活，轰炸期间会造成用户无法正常使用手机，请谨慎使用。
		RiskWare/Android.B4ASmsSend.e[exp]	中	该应用程序是测试程序，包含风险代码，可以接收远程指令执行发短信、定位等操作，存在一定的风险，请谨慎使用。
		RiskWare/Android.Algo360.a[prv]	中	该应用程序为金融相关应用，以评估用户信用的名义，获取用户位置、短信、联系人、通话记录等隐私信息，建议用户谨慎使用。
		RiskWare/Android.61bocai.a[rog]	低	该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	OpenType 字体分析远程代码执行漏洞（CVE-2019-1419）	高	当 Windows Adobe Type Manager 库未正确处理经特殊设计的 OpenType 字体时，会触发远程代码执行漏洞。对于除 Windows 10 之外的所有系统，成功利用此漏洞的攻击者可以远程执行代码。对于运行 Windows 10 的系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在 AppContainer 沙盒中执行代码。攻击者可随后安装程序；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	Trojan[Backdoor]/Win32.Jaan	中	此威胁是一种带有后门的木马类程序。该病毒家族通过另一个木马下载运行。该家族木马可以执行指定命令，下载任意文件。
		Trojan[PSW]/Win32.Meger	中	此威胁是一种具有窃取密码行为的木马家族。该家族的样本在执行后会监视用户的键盘输入，并将用户输入的密码发送给远程的控制端。
		Trojan[Banker]/Win32.Dyre	中	此威胁是一种以窃取网络银行敏感信息（如银行账号、密码、信用卡信息等）为目的的木马类程序。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给黑客。
		Trojan/Win32.Ruvs	低	此威胁是一种木马类程序。该家族样本伪装成系统进程，拖慢计算机速度。
		Trojan/Win32.SmallGame	低	此威胁是一种木马类程序。该家族样本运行后修改浏览器默认页面，弹出广告，重定向网页到其他网址。

5G IoT 安全：机遇与风险并存

Zeljka Zorz/ 文 安天技术公益翻译组 / 译

虽然缓慢但是可以肯定，5G 数字蜂窝网络正在全球范围内建立。

要实现广泛的 5G 覆盖并加以使用，还需要数年的时间。因此，何不趁现在寻找一种既能够轻松使用 5G 网络又能够确保安全性的方法呢?

机会与风险并存

“毫无疑问，5G 会打开一个全新的世界，为用户提供更高速度和更低延迟的服务。但是，随着这种技术进步，用户和网络运营商也会面临更大的风险。”NETSCOUT 首席技术官达伦·安斯第（Darren Anstee）在接受 Help Net Security 采访时说。

对于网络运营商来说，5G 架构将会很复杂。支持新服务所需的多路访问边缘计算，将促使更多的供应商采用移动基础架构；而支持服务“切片”的基础架构将被虚拟化或容器化并进行编排。管理服务和端点连接的控制面板，其复杂性也增加了。伴随着这种复杂性，被感染或运行不佳的设备或应用程序可能会带来安全问题。

对于消费者而言，隐私是一个大问题。5G 的主要用途之一是“大规模机器类型通信”（mMTC），这会导致大量低功耗、低成本 IoT 设备的持续扩散，因此信息收集和交换将会增加。

企业将能够收集我们在线 / 离线活动的大量信息，从而更详细地了解我们的行为。安斯第表示，这将促使企业针对消费者的需求、位置和习惯为其量身定制服务，但很可能会引发针对个人及其所在公司的新一波社会工程攻击。

消费者担忧的另一个问题是：即使用户数据是匿名的，企业通常也可以为用户构建虚拟身份，并利用这些数据驱动分析和其他决策系统。

“在这方面，需要进一步完善监管。随着数据收集越来越普遍，分析越来越智能，个人用户需要加强防护，以免受到突如其来的攻击。这些攻击根本不在意受害用户的真实身份是什么，有一个虚拟的身份标识就够了。”

5G IoT 安全隐忧

预计在 2021 年之前，mMTC 网络不会广泛部署。但其广泛部署是迟早的事，届时会为企业、公共实体、工业环境等广泛使用 IoT 设备铺平道路。

设备连接和互联的规模不断扩大，再加上“切片”（针对特定应用程序或服务的独立虚拟移动网络，其特征取决于应用程序或服务需求）的概念，必将带来一系列新的 IoT 服务和应用程序，安斯第说。

其中一个安全漏洞是设备本身。大多数现有的 IoT 设备在开发时都未将安全性作为优先考虑因素。

“并非所有 IoT 设备都‘生而平等’，对消费者设备和工业设备应区别对待。后者往往设计得更好，安全性更高，并且在许多情况下将连接到特定的网络切片或通过 IoT 网关设备连接——这消除了进行常规扫描和破坏活动的可能性。”他解释说。

“但是，这些设备可能对任务或安全至关重要，其感染或故障可能会造成严重的后果。因此，必须对它们进行监控以确保其像预期一样运行。”

我们与多家希望推出 5G 的网络运营商进行了交谈，他们都表达了对消费者 IoT 设备的担忧。

“针对有线连接的 IoT 设备的大规模 DDoS 攻击很普遍，没有迹象表明连接到 5G 网络的 IoT 设备的情况会更好——这是因为未考虑到安全性或安全性较差的新设备仍在部署，而已部署的设备将运行多年。”他补充说。

“大量易受攻击的、5G 连接的 IoT 设备会产生大量流量，并且它们的动作同步性可能会耗尽基础架构某些方面的资源，从而对移动网络构成威胁。”

针对 CISO 的建议

保护依赖 5G 的企业 IoT 网络，将是一项复杂的任务。

“鉴于我们讨论的设备类型和用途非常广泛，因此没有针对 CISO 的简单、通用建议。电梯、联网汽车、医疗传感器和工业机器人在用途、所需的通信服务类型、软件堆栈、流量模式等方面有很大的不同。在对安全性的潜在影响方面（从个人或环境安全的角度），也有很大的不同。”安斯第指出。

“此外，不同类型的设备通过不同的销售渠道提供，并由不同的企业进行维护，因此存在很多变量。”

但是，我们可以采取一些基本措施，保护设备免受大多数常见攻击和大规模恶意软件。

- 选择可以为设备提供持续支持和软件更新的供应商 / 制造商。
- 尽可能使用最新的软件，并建立适当的流程来评估已披露 / 发现的新漏洞，以便对其进行适当管理。
- 采用可见性解决方案或服务，以便对设备的行为进行概要分析和监控，以发现和调查异常行为。

在工业环境中利用 5G 驱动 IoT 自动化的企业，可能会将各种网络切片用于不同的服务。他们必须确保其移动服务提供商在其网络内进行适当的监控，以监督对这些切片进行访问的联网设备和基础架构的活动。

“管理 5G 网络和服务的安全性（端到端架构不可或缺的一部分）需要一种新方法。安全不仅要依靠确保移动网络内协议一致性的防火墙，还要依靠在 Internet 边缘（将移动核心网络连接到 Internet 主干网的 SGi 接口）提供入站和出站威胁检测的其他解决方案。”

“在 5G 网络中，我们需要在整个网络中保持一致的可见性，以便识别针对控制面板、用户面板、端点、服务或应用基础架构的威胁，并确保在网络内部识别和修复威胁，从而保护网络、服务和用户。最后，提供这些可见性和威胁管理功能的技术，需要与虚拟化或容器化基础架构集成，以便将它们的生命周期和扩展性关联起来。”

原文名称	5G IoT security: Opportunity comes with risks
作者简介	Zeljka Zorz。Zeljka Zorz 是 Help Net Security 的总编辑。
原文信息	2019 年 12 月 2 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/12/02/5g-iot-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。