安天发布《Ryuk 勒索软件分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一种名为 Ryuk 的勒索软件木马。Ryuk 于 2018 年 8 月首次出现，与其他许多勒索软件系列不同，它以一种更新颖的方式感染系统。

Ryuk 首次出现于 2018 年 8 月，虽然在全球范围内并不是非常活跃，但至少有三个组织在其头两个月的行动中遭受了 Ryuk 的感染，攻击者获得了大约 64 万美元的赎金。Ryuk 本身拥有其他现代勒索软件系列中可以看到的功能，包括识别、加密网络驱动器和资源以及删除端点上的卷影副本等。通过这样做，攻击者可以禁用 Windows 系统还原选项，使用户无法在没有外部备份的情况下从攻击中恢复。攻击者通过弱 RDP（远程桌面协议）密码进入受害者的网络，提权成为管理员，卸载安全软件，最后加密用户文件。研究人员认为 Ryuk 是通过僵尸网络（如 TrikBot 和 Emotet）作为二级有效载荷进行传播。TrikBot 与 Emotet 都被用作信息窃取，下载恶意代码。可以猜测，Ryuk 的目的可能是在信息窃取之后，用以榨取更多价值。

安天 CERT 提醒广大政企客户，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

目前，安天追影产品已经实现了对该类恶意代码的检出。

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、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、动态（Win7 x86）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	de708f2807f96938e5eb0295d5ebfee870b34dd0cb70708607d4e1adf767ce7b
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	148 KB
MD5	3C5575CE80E0847360CD2306C64B51A0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=3C5575CE80E0847360CD2306C64B51A0

◆ 运行环境

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

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	138	192.168.122.255	138
192.168.122.155	138	192.168.122.111	138
192.168.122.111	137	192.168.122.155	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	137	192.168.122.255	137
192.168.122.111	123	52.173.193.166	123
192.168.122.1	67	192.168.122.111	68

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1032	192.168.122.155	139

◆ 运行环境

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

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	59175	192.168.122.1	53
192.168.122.165	53769	192.168.122.1	53
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 01 月 21 日 (总第 169 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天态势感知平台获“金帽子”年度优秀安全产品奖

1 月 15 日，2018 网络安全“金帽子”奖年度盛典在北京举行。安天态势感知平台获年度优秀安全产品奖。

由公安部第一研究所指导、嘶吼传媒主办的“金帽子”奖评选大会聚集众多国内安全专家、学者、白帽子、媒体舆论领袖等上百名嘉宾，共同评选并答谢 2018 年对行业做出杰出贡献的网络安全组织及精英们。

本次评奖活动共包含八大奖项，分别为业内评选的四个奖项和大众评选的四个奖项。其中业内评选奖项，由五十位安全专家组成的评审团进行评审工作；大众评选奖项，由业内外广大人民群众通过新闻、微信、微博等多渠道参与投票评选。评选活动全程历时 75 天，经组委会严格审核，共预选了近百个项目入围。最终，安天态势感知平台获得了评审专家们的一致认可，荣获年度优秀安全产品奖。

态势感知在积极防御体系中对于提供响应决策、支持保障业务弹性和风险控制至关重要。但当前在态势感知实践中，往往更偏重于面向策略调整的宏观态势感知，难以支撑有效积极防御体系。面向实战化运行的战术型态势感知能够为威胁对抗行动提供实时监控响应能力，指挥对网络潜伏威胁进行猎杀清除，在攻防时间周期上适应高速多变的攻击行动，提升网络安全防护工作的积极性和主动性。

安天为重要信息系统和关键信息基础设施提供面向实战化运行的战术型态势感知解决方案，全面覆盖了网络和信息化基础设施各个组成实体，实现全生命周期的资产集中安全运维；通过将威胁知识与客户专有多源安全数据结合，配套高阶威胁情报与持续追溯服务，持续将威胁应对经验转换为客户的防护与响应能力。

新加坡数据泄露事件涉及微软 Outlook 漏洞

官方调查发现，在去年新加坡 150 万名医疗保健患者（包括总理）个人数据泄漏事件中，攻击者使用公开可用的黑客工具利用了微软 Outlook 中的一个已知漏洞。该恶意网络活动的持续时间超过 10 个月，在新加坡居住的每 4 个人中就有 1 人的个人数据被泄露，包括地址和身份证号码。根据调查，大约有 159,000 人的门诊药物记录已被公开。报告称，攻击者有一个明确的目标，即新加坡总理李显龙和其他患者的个人和门诊药物数据，并且攻击活动具有民族国家支持团体的特征。

（来源：https://www.cyberscoop.com/apt-heist-singapore-health-data-exploited-microsoft-outlook-inquiry-finds/）

研究人员发现利用 Java Script 传播的垃圾邮件活动

自 2018 年 12 月 31 日以来，研究人员发现超过 72,000 封垃圾邮件，传播至少 8 种类型的恶意软件，如 GandCrab、Smoke、AZORult、Phorpiex 以及一些挖矿软件。其中大部分目标是教育、政府、制造业和银行业。与随机电子邮件地址不同，用户只要单击垃圾邮件附加的 ZIP 文件就会触发 JavaScript，进而从 C2 下载恶意软件。垃圾邮件活动激增使得研究人员收集到大量哈希，追溯到俄罗斯的 IP 地址已经不能访问，但是有效载荷可以在线获得。攻击者可以更改 .EXE 文件中包含的恶意软件，并根据所针对的地区和行业传播不同类型的恶意软件。

（来源：https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/javascript-malware-in-spam-spreads-ransomware-miners-spyware-worm）

每周安全事件

类 型	内 容
中文标题	广告软件伪装成应用程序感染了 900 万谷歌用户
英文标题	Adware Disguised as Game, TV, Remote Control Apps Infect 9 Million Google Play Users
作者及单位	Ecular Xu
内容概述	趋势科技研究人员发现一个活跃的广告软件活动，广告软件在 Google Play 商店中伪装成 85 个游戏、电视和遥控模拟器应用程序。这些应用程序已在全球共下载了 900 万次，能够显示全屏广告并隐藏自身，监控设备的屏幕解锁以及在移动设备的后台运行。研究人员测试了与广告软件系列相关的每个假应用程序，发现这些应用虽然来自不同的制造商并且具有不同的 APK 证书公钥，但它们表现出相似的行为并共享相同的代码。
链接地址	https://blog.trendmicro.com/trendlabs-security-intelligence/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users/

每周值得关注的恶意代码信息

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 平台的恶意代码值得关注

关注方面		名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.mobStspy.a[prv,rmt,spy] 2019-01-15	该应用程序是一款间谍软件，接收远程控制指令，弹出钓鱼界面诱导用户填写相关信息，窃取用户短信、联系人、地理位置、通话记录、手机文件、社交软件记录等隐私信息，并上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Burkl.a[exp,sys] 2019-01-16	该应用程序包含风险代码，运行后联网获取广告数据，私自加载广告，下载 root 子包提权。造成用户流量消耗，危害用户手机安全，建议卸载。（威胁等级高）
		Trojan/Android.SmsListener.w[prv,exp] 2019-01-07	该应用程序运行后拦截用户短信，窃取用户短信并将其发送到指定手机，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Tool/Android.CJZCH.c[sys]	该应用程序是一个游戏修改工具，会修改游戏参数，部分功能需要 root 权限，请谨慎使用。（威胁等级低）
		RiskWare/Android.RYbocai.a[rog]	该应用程序是线上博彩游戏，其内容可能给用户的财产带来较大风险，且难以保障财产权益，请谨慎使用。（威胁等级低）
		RiskWare/Android.Joke.f[rog]	该应用程序是整蛊程序，无实际功能，运行后会显示色情图片，同时播放音乐，修改用户桌面壁纸，建议立即卸载。（威胁等级低）
		Trojan/Android.SPPSpy.a[prv,rmt,spy]	该应用程序伪装政府类应用，运行后接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置等信息，监听用户短信和通话，私自发送短信、拨打电话，显示虚假钓鱼界面。造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Ware/Android.FakeSexApp.j[rog,exp]	该应用程序伪装色情应用，本身无实际功能，诱导用户分享、加群，访问代刷类网站，诱导下载风险、骗钱类应用，存在较大的风险，建议不要使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows 权限提升漏洞（CVE-2019-0543）	当 Windows 内核无法正确处理内存中的对象时，可能就会触发该漏洞。攻击者首先必须登录到系统。然后运行一个经特殊设计的应用程序，才能利用此漏洞。成功利用该漏洞的攻击者可以在内核模式中运行任意代码。攻击者可任意安装程序，查看、更改或删除数据，或者创建新帐户等。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/MSIL.AGeneric	此威胁是一种具有下载行为的风险软件类程序。该家族会自动下载并运行用户不知情或不允许安装的软件，同时它也可以不断地检查更新文件本身。（威胁等级中）
		Trojan[Clicker]/JS.FbLiker	此威胁是一种可以实施自动点击功能的木马家族。该家族样本是 JS 脚本编写，可以模拟点击攻击者设定的网址中的广告。（威胁等级低）
		Trojan[Downloader]/Win32.Tolsty	此威胁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至服务器。（威胁等级中）
		HackTool[Hoax]/MSIL.ArchSMS	此威胁是一种可以对用户实施恶作剧的、利用微软中间语言 MSIL 编写的黑客工具家族。该家族样本是加密的压缩包，运行后要求用户向某个号码发送短信以获取解压密码，在短信发出后，可能有三种情况：什么都没有发生、解压后的文件与其声明的不同、解压的文件是推广应用。（威胁等级中）
		GrayWare[AdWare]/MSIL.Agent	此威胁是一种用 MSIL 语言编写的灰色软件程序。该家族并没有统一的行为与功能，而是像一个灰色软件类程序集合一样，将大量以基因片段定性的恶意代码归类。（威胁等级低）

物联网向构建智能边缘计算平台转型

Kevin Meany/ 文 安天技术公益翻译组 / 译

当你需要数据时，它们在哪里呢？“边缘计算”（edge computing）为处理云端或数据中心的所有数据提供了一种替代方案。

随着物联网（IoT）的出现，企业被越来越多的数据淹没。其中，大部分数据被上传到云端，以便随时随地从任何设备进行访问。云中数据的指数级增长导致了一系列问题，特别是安全问题，例如，确定“谁”应该具有访问权限，具备“什么”级别的访问权限等。此外，云还存在延迟问题——企业需要实时访问数据，而云可能会导致访问延迟。

“边缘计算”应运而生，并保持着强劲的上升势头。随着大数据工作负载和实时计算的增长，云中的计算被不断拖慢；因此，企业迫切需要转向边缘计算。边缘计算是指具有分散处理能力，支持移动计算和 IoT 技术的开放 IT 架构；通常涉及位于智能产品附近的服务器，这些服务器收集数据并对其进行计算。在边缘计算中，数据由设备本身或本地计算机处理，而非传输到数据中心 / 云端进行处理。

这给企业带来了其他挑战。例如，如何确定在近期、短期或长期（存档）访问哪些组织和运营数据，以及如何为这些数据创建适当的存储库等。

企业可以从现场的数十亿台设备中收集大量的数据，而是否关注“细节”——例如影响企业实施 IoT 方案的行业法规和最佳实践——决定着企业的成败。

例如，在石油和天然气行业中，海上石油平台并不具备最佳的互联性，但它们需要处理跟踪钻井性能的大量数据。这些数据被保存，通常不会立刻进行分析，而是在之后被查看。在一些情况下，如果手头有可用的数据，可以直接调整钻井的阀门。由此可见，在实时访问关键数据方面，边缘计算系统非常有价值。

物联网还可以用于医疗领域，例如心脏和患者监护仪、超声波、癌症治疗计划系统和各种智能医疗设备。随着医疗数据的迅速增加，将所有数据传输到云端或数据中心进行处理的效率很低，因此边缘计算在医疗领域的价值更加突出。

边缘计算也可以用于零售店铺的实时购物，即通过产品或人脸识别处理购物。在这种情况下，生成的数据流很大，将所有数据上传到云端进行处理速度很慢，而且成本很高。然而，边缘计算可以解决这些问题。例如，一些自助餐厅已经开始利用边缘计算进行结算。

那么，从边缘计算转型中获得最大收益的最佳途径是什么呢？从 IoT 设备收集（通常是实时收集）的信息，可以为企业的每个层级提供新的见解。通过传播和分析大数据，IoT 能够为企业带来巨大的价值。企业可以获得很多收益，但他们应该如何确定哪些收益能够带来最佳业务成果呢？

首先，企业应确定需要远程（例如在海上石油平台）访问和使用的数据，这一点至关重要。边缘计算在数据源附近高效地处理数据，可以减少对互联网带宽的占用。这样不仅能够降低成本，还能够确保有效地对应用程序进行远程访问。此外，这还能为敏感数据提供一定程度的安全性和隐私性。

成功的边缘计算转型需要关注敏捷性和性能。例如，一台边缘设备无法提供企业数据中心所需的计算能力或存储能力。这需要多台边缘设备创建一个平台，该平台能够收集数据，但是收集数据的速度和量不会超过云或公司移动网络的承受能力。该平台还能够提供用户特定的数据，用于制定更好的运营或业务决策，即预测威胁或提供告警。此外，该平台还能够提供实时情境数据（即实时发生的情况），以及高水平的安全性。

有几家公司可以提供应用程序，如 HPE Aruba，Nutanix，微软 Azure 和亚马逊，帮助企业定义和启动边缘智能平台。边缘计算策略以智能平台为基础，以云为长期存储、分析和机器学习的存储库。通过聚合来自边缘设备的数据，企业可以利用云来更好地理解数据模式和趋势。

原文名称	IoT: Living on the Edge
原文作者	Kevin Meany.Kevin Meany 是 Versatile 公司的联合创始人兼首席技术官。
原文信息	2018 年 12 月 31 日发布于 InformationWeek 原文地址 https://www.informationweek.com/strategic-cio/it-strategy/iot-living-on-the-edge/a/d-id/1333561
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。