安天发布《Wirenet 木马样本分析报告》

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 Wirenet 的挖矿木马。该木马以 Opera、Firefox、Chrome、Chromium 等跨平台浏览器和 Thunderbird、SeaMonkey、Pidgin 等应用的密码为目标，窃取用户信息。

Wirenet 在 Linux 平台下会自动复制至“~/WIFIADAPT”目录，然后使用 AES 加密通道，连线至 C&C 服务器。该样本的函数数量较多，大部分的字符串信息已经被加密，样本在网络传输过程中使用了 AES 加密。因此，样本 main 函数执行时首先进行了 AES 的初始化操作，其使用的 AES 加密模式为 CFB。其次，样本 main 函数中还调用了一个 InstallHost 函数用于执行自我安装程序，同时在 ReadSettings 函数中包含了一些设置的重要信息。样本的重要信息都采用 RC4 加密方式进行加密，通过 GDB 动态调试即可获取到大量信息，如连接的服务器、密码等，这些信息在 InstallHost 函数中被使用，而 InstallHost 函数中的 Wirenet 使用解密出的信息与服务器建立连接，并且在 /.config/autostart 中设置开机自启动功能。另外样本中还有一个重要的函数 ProcessData，通过对 ProcessData 函数的调用关系可发现，该函数包含了大量功能，如遍历文件夹、读写文件、获取操作系统版本和用户信息、鼠标监控、开关机等，Wirenet 基本具备了一个普通后门程序所具备的功能。

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、文件来源信息鉴定器、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、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器、安全云鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	35ff79dd456fe3054a60fe0a16f38bf5fc3928e1e8439ca4d945573f8c48c0b8
文件类型	BinExecute/Linux.ELF
大小	63 KB
MD5	9A0E765EECC5433AF3DC726206ECC56E
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Wirenet
判定依据	安全云

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=9A0E765EECC5433AF3DC726206ECC56E

◆ 运行环境

操作系统	内置软件
中标麒麟	默认

◆ 危险行为

行为描述	危险等级
自复制	★★★★★
修改文件权限	★★

◆ 病毒百科

Trojan	这是一种具有危害主机安全特性，能实现窃取关键信息、数据破坏等恶意功能的代码。但原则上没有感染其他文件能力的恶意代码。其中也包括一些为实现相关恶意功能的工具。
Backdoor	攻击者利用后门可以远程控制受害者的电脑。后门允许攻击者在被感染的电脑，做任何操作如发送 / 接收 / 打开 / 删除文件，删除用户的数据，弹出消息，并重新启动计算机。

◆ 检出行为

危险行为	自复制
常见行为	修改文件权限

◆ 常见行为

安天周观察
安天官方微信
主办：安天 2019 年 01 月 07 日 (总第 167 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天网络安全冬训营历年主题回顾

自 2014 年起，在相关领导部门和职能机构指导下，安天已经连续成功举办了五届网络安全冬训营，并提出了“直面实际威胁，形成价值落地”的活动导向。从 2016 年开始，为了让议题和内容更为聚焦，安天将冬训营主题化，决定将每一届冬训营围绕一个核心主题进行。本期周观察将为您梳理历届网络安全冬训营的主题脉络，与您一起重温历届冬训营的精彩盛况。

2014 年 第一届安天网络安全冬训营：“凛冬将至”

2014 年年初，安天举办了主题为“凛冬将至”的第一届网络安全冬训营，我们选择“冰与火之歌”中这句有着象征意义的词句，因为这正是我们对整个网络安全威胁全面泛化的发展趋势的预言，而大国博弈所带来的网络安全大竞革的时代也才刚刚开始。本期议题包括国际网络安全态势、工控安全方向、移动安全新趋势与黑色产业链发展、WEB 安全方向等内容，得到了很多业内专家和网络安全技术爱好者的支持。

2015 年 第二届安天网络安全冬训营：“北风乍起”

“北风乍起”既是对 2014 年网络威胁全面泛化趋势的总结，也是对 2015 年安全行业将要迎接挑战的预期。在本届冬训营中，来自网络安全主管单位的专家学者和国内网络安全公司的一线研究人员在为期三天的会议中进行了精彩的演讲，议题包括操作系统、移动安全、病毒分析、应急响应等内容，会议为网络安全领域学生和爱好者提供了接触网络安全实战，了解网络安全最新技术的沟通平台。

2016 年 第三届安天网络安全冬训营：“朔雪飞扬”

2016年安天网络安全冬训营再次起航，本期冬训营以“情报的支撑，塔防的实践”为核心议题，一如既往地专注检测防御，依然坚持对追求工程能力的信念。我们期待威胁情报不止是一个热点，我们期待塔防纵深防御模型形成更具体的实践指导。在“朔雪飞扬”中，冬训营为网络安全保卫者与爱好者提供了一个分享、交流的机会和平台。

2017 年 第四届安天网络安全冬训营：“冰峰屹立”

第四届安天网络安全冬训营——“冰峰屹立”围绕“有效防护，价值输出”这一主题展开，旨在自我批判我们作为安全厂商和研究者的主观局限和技术优越感，回归安全技术为用户提供有效的防护能力和价值保障的本质。我们搁置种种名词、理念的争论；我们透过各种热点的迷雾，以专业务实的态度，深入挖掘用户的真实安全需求，为安全技术、产品与服务实现有效的客户价值寻找落地方式，探寻可实施的解决方案。

2018 年 第五届安天网络安全冬训营：“红旗漫卷”

第五届安天网络安全冬训营——“红旗漫卷”以“敌情想定是前提，网络安全实战化”为主题，旨在打破旧有以“物理隔离 + 好人假定 + 规定推演”构成的自我麻痹式的安全观，以真实的敌情想定为前提，以实战化作为网络空间安全防御的第一要求，让安全技术、产品与服务能够随时应对真实的威胁，为客户实现有效的安全价值。

第六届安天网络安全冬训营“铁流鏖战”将于2019年1月8、9两日在哈尔滨举行，本届冬训营将以“战术型态势感知指控积极防御，协同响应猎杀威胁运行实战化”为主题，敬请期待。

详情请登录冬训营官网 http://wtc.antiy.cn/

每周安全事件

类 型	内 容
中文标题	欧盟将开启 15 个免费开源软件漏洞奖励计划
英文标题	In January, the EU starts running Bug Bounties on Free and Open Source Software
作者及单位	Julia Reda
内容概述	欧盟发布了今年在免费和开源软件中 14 项被发现漏洞的奖励计划，并将在明年继续执行，共开启 15 个软件漏洞奖励计划，总奖励额达 85 万欧元。欧盟表示发现漏洞者可以通过分析软件以及向所涉及的漏洞赏金平台，提交发现的任何漏洞。奖金的数额取决于所发现问题的严重性和软件的相对重要性。所选择的软件项目包括在以前清单和公众调查中被确定为候选的项目。
链接地址	https://juliareda.eu/2018/12/eu-fossa-bug-bounties/

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.mestheft.a[prv,rmt,spy] 2018-12-29	该应用程序伪装系统服务，运行后请求 root 权限，接收远程控制命令，窃取用户短信、联系人、地理位置、手机文件及手机各项基本信息，监听用户通话，私自拍照、录音、录像，记录用户键盘录入和截屏信息。并将用户隐私上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.by1cspy.a[prv,exp,spy] 2018-12-30	该应用程序伪装系统应用，运行后会获取 root 权限，接收远程指令，锁屏勒索。私自下载安装 apk，模拟点击支付，通过模拟点击窃取用户 QQ、微信和转账支付等信息。窃取用户短信、通讯录、手机号码，获取相机权限，拍摄照片视频，私自发送短信，造成严重的隐私泄露和资金损失，建议立即卸载。（威胁等级高）
		Trojan/AndroidSMSReconSpya[prv,exp,rmt,py] 2018-12-31	该应用程序伪装正常应用，实际是重打包间谍工具，会接收指令，上传用户录音、照片、信箱、通讯录、位置等隐私信息，删除存储文件、修改手机设置，会造成用户隐私泄露，影响用户正常使用，建议立即卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.BKspy.c[prv]	该应用程序伪装热门应用，无实际功能，拦截短信，后台通过发送邮件的方式私自窃取用户短信、联系人信息，造成用户隐私泄露，建议卸载。（威胁等级低）
		RiskWare/Android.KingkrProgram.a[exp]	该类应用程序是在线生成的，大多是色情、博彩、代刷代挂、刷赞类应用，存在一定的风险，请谨慎使用。（威胁等级低）
		RiskWare/Android.tcFuzhu.a[rog]	该应用程序通过工具生成，运行后会请求 root 权限，可能存在风险，请用户谨慎使用。（威胁等级低）
		Trojan/Android.MTruss.b[pay]	该应用程序运行后会私自发送短信到指定号码，短信内容为用户手机固件信息，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.inspicySms.a[exp,prv]	该应用程序伪装病毒清理应用，运行后激活设备管理器权限，窃取用户手机 SIM 卡信息、型号、运营商、ID 号、手机固件信息、手机软件安装信息，联网获取短信数据，私自发送短信，@ 造成用户资费消耗和隐私泄露，建议立即卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 权限提升漏洞（CVE-2018-8641）	当 Windows 内核无法正确处理内存中的对象时，可能会触发该漏洞。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	Trojan[Rootkit]/Boot.Sinowal	此威胁是一种可以窃取用户信息的木马家族。该家族具有 rootkit 功能，可以修改 MBR 并在系统内核运行之前加载，难以被发现和清除。（威胁等级高）
		GrayWare[AdWare]/Win32.CrossRider	此威胁是一种有广告行为的灰色软件类程序。该家族有安装捆绑软件、修改浏览器主页和默认搜索引擎等恶意的行为。（威胁等级低）
		Trojan[Downloader]/JS.Twetti	此威胁是一种使用 JS 脚本编写的可以下载其他恶意代码的木马家族。该木马家族会向 Twitter 的 API 发送请求，利用其接收到的数据生成随机名称的域名。感染者会被重定向到这些域名。攻击者注册此域名，然后将恶意程序放置在这些网站上，用来感染更多计算机。（威胁等级中）
		Trojan/Win32.Lunam	此威胁是一种木马类程序。该家族运行在 32 位平台下，会在受感染计算机的指定目录下复制自身，导入注册表。会收集用户信息并可以感染移动设备。（威胁等级中）
		Trojan[Backdoor]/Win32.Spammy	此威胁是一种可以窃取用户信息的木马家族。该家族运行后会搜索感染者电脑 Outlook 通讯录中的联系人列表和互联网资源管理器缓存文件中的电子邮件地址，并将收集到的信息发送至黑客指定的服务器。该病毒家族还会读取黑客预先放置在远程服务器上的文件，并按照该文件内容，向感染者的联系人发送垃圾邮件。（威胁等级中）

构建可扩展的 IR 自动化和编排计划：三个关键点

Brenden Glynn/ 文 安天技术公益翻译组 / 译

事件响应（IR）自动化和编排计划对于网络安全至关重要。该计划能够自动化地执行流程，最大限度地提高资源功效和企业的整体安全态势，从而减轻安全专家的负担。随着安全告警数量的急剧增加和技能差距的不断扩大，安全团队迅速采用 IR 自动化和编排解决方案，希望能够迎头赶上。市场分析机构 Enterprise Strategy Group 指出，近 85% 的企业已经采用或正在采用这些解决方案。

制定适合企业的、强健的 IR 计划

尽管采用自动化和编排解决方案的企业不断增加，但是，成功实施这些解决方案并不像部署它们那样简单。首先，安全团队需要制定强健的 IR 计划——如果想要自动执行流程，需要先定义这些流程。

IR 手册（企业针对各类事件的响应行动和任务）是 IR 计划的核心。无论企业是从头开始构建 IR 计划，还是采用高级编排工具，记录在案的 IR 流程都是基础。在考量一些关键因素的基础上，安全团队可以构建在未来很长时间内为企业带来收益的 IR 手册。

以下是构建强健、一致的 IR 计划的三个关键点。

1. 围绕手动任务构建初始手册

无论外部技术的功效如何，良好的 IR 手册都应该起到作用。该手册记录分析师在 IR 流程中需要执行的全部任务，并对未来的编排和自动化进行规划，以协助分析

师在事件发生期间制定决策和采取行动。

这些手动任务应该以行动为导向，并且具有可测量的目的和结果。手册应尽可能地向分析师提供执行某项任务的“原因”，并详细地描述任务。这样一来，分析师可以轻松验证流程，并在团队中上下传递这些流程。此外，企业应创建培训机会，促进内外部审计的顺利进行。

2. 持续评估和精简流程

IR 是一个持续改进的过程，因此，IR 手册应该不断维护和改进，例如根据模拟和现实操作习得的经验，来替换或删除某些任务。

企业应该考虑如何存储、使用和维护手册。无论手册是什么格式（纸质版、电子版、业内知识），更新和传播 IR 手册都是颇具挑战性的。集中且安全的平台（例如内部 wiki 或文档共享）可以实现更好的协作管理，而 IR 平台可以在事件发生之前、期间和之后实现无缝协作。

反馈循环，也称为“事后分析过程”或“事后回顾”（AAR），对于企业减少响应时间和提高运营效率至关重要。此外，为了编排和自动执行某些用户任务和行动，企业需要获取经过验证的指标，以便了解哪些流程应该实现自动化，并衡量自动化的影响和投资回报率（ROI）。我们将在后续博文中给出这些指标的示例。

3. 手册应该是迭代和可扩展的

随着 IR 计划的发展，企业希望能够快速开发针对其他事件类型或场景的新手册，以适应威胁形势的变化并更改现有手册的范围。

企业可以确定常见的流程和任务，将其分配到各个模块中，并在所有手册中共享这些信息，从而提高手册应用和维护的灵活性。

当然，如果出现了新的流程，可以创建和维护与该流程有关的具体、详细的工作内容。随着技术、技能、要求和资源的变化，企业可以快速调整现有的模块化流程来解决这些问题，而无需对多个不相关和可能重复的任务进行编辑。

企业可以重用这些常见的任务和模块化流程，而无需从头开始构建新手册——因为这将是一项繁琐和低效的工作。

为今后的成功奠定基础

强健的、记录在案的 IR 计划是成功实施自动化和编排计划的基础，而关注细节、促进应用灵活性、强健且可扩展的 IR 手册将为企业带来多年的收益。

原文名称	3 Keys to Building a Scalable Incident Response Automation and Orchestration Plan
原文作者	Brenden Glynn.Brenden Glynn 是一位网络安全事件响应专家，担任 IBM Resilient 公司的事件响应顾问。
原文信息	2018 年 12 月 14 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/3-keys-to-building-a-scalable-incident-response-automation-and-orchestration-plan/
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。