安天发布《ZombieBoy 挖矿木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 ZombieBoy 的木马。该木马最早出现于 2017 年底，分析人员监测到该木马目前已经在多个行业迅速扩散，其中，企业为感染的重灾区，教育行业和政企单位等均受到不同程度的感染。ZombieBoy 木马包含了内网扫描、“永恒之蓝”漏洞利用、“双脉冲星”后门、挖矿工具等多个恶意模块，是一款集端口扫描、远控、挖矿功能为一体的混合型木马。

ZombieBoy 运行后，会在 windows 目录下创建一个随机 5 位字母的文件夹，并在该文件夹下释放“永恒之蓝”工具包、端口扫描工具和“双脉冲星”后门植入工具。创建 aC.exe 挖矿程序，下载 123.exe 到 C:\\Windows\\System32\\sys.exe，并运行。访问 http://v9.monerov8.com:8800/A.txt 获取 URL 地址用于下载恶意文件，当前木马的 URL 已失效。接下来该木马从自身释放并执行 84.exe、创建脚本文件 SB360.bat 到 windows 目录下和下载执行 wk.exe 并将其重命名为 CPUInfo.exe。84.exe 的主要功能是检测是否存在名为 dazsks gmeakjwxo 的服务，没有就创建该服务、删除自身和解密 C2 地址等。创建脚本文件制定 IP 策略，屏蔽 135、139、445 等端口。CPUInfo.exe 的功能是运行挖矿进程。感染该挖矿木马后清除比较麻烦，同时会出现内网传播的情况。

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。确保所有的计算机在使用远程桌面服务时避免使用弱密码，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该类木马的鉴定；安天智甲已经实现了对该木马的查杀。

黑客工具

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述黑客工具进行有效检测，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、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、反病毒引擎鉴定器、动态行为鉴定器、信标检测鉴定器将文件判定为黑客工具。

◆ 概要信息

文件名	9a008c505fa37e50a4c6f91f27a99c710442e250cb23886eb40f5d8ff721593a
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	804 KB
MD5	263584AF66662C6589D8D646E15965F7
病毒类型	黑客工具
恶意判定 / 病毒名称	HackTool[VirTool]/Win32.Ceeinject
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=263584AF66662C6589D8D646E15965F7

◆ 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

◆危险行为

行为描述	危险等级
通过 CMD 隐藏删除自身	★★★★
延时	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
获取系统版本	★
创建窗口	★
加载运行时 DLL	★
获取系统信息(处理器版本、处理器类型等)	★
连接网络	★
释放 PE 文件	★
创建挂起进程	★★
壳行为填充导入表	★★
自复制到系统目录	★★
设置文件属性为隐藏	★★
隐藏 PE 文件	★★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 08 月 12 日 (总第 195 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

中国航天科技集团副总经理杨保华一行莅临安天总部交流合作

8 月 1 日，中国航天科技集团副总经理杨保华，集团科技委主任、中科院院士包为民、集团科技委秘书长王晓军一行莅临安天总部交流合作，与安天集团负责人肖新光等人进行了深入研讨。

参观中，来宾们详细了解了安天的整体研发能力、核心引擎能力、产品体系和解决方案，重点听取了安天在安全解决方案中“安全运维一体化”的思路。安天相关负责人向来宾们展示了战术型态势感知平台的研发进展，介绍了“白象”、“绿斑”、“方程式”等具有代表性的高级网空威胁行为体及超高能力网空威胁行为体的支撑体系、攻击装备、作业特点等，对一些典型攻击活动按照网空威胁框架进行了复盘演示。

在讲解过程中，相关负责人表示，面对体系化的网空攻击行为，仅靠物理隔离难以在网络空间有效对抗高能力对手的威胁。对于关键信息基础设施和重要信息系统等防御场景，应以“敌情想定”为前提，采用叠加演进能力导向的网络安全建设模式指引规划设计，科学合理地分阶段扎实开展网络安全建设实施工作，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的网络安全能力，构建动态综合的网络安全防御体系。

来宾对安天的核心技术能力表示高度认可。双方就战略合作进行了深入讨论。

微信扫描二维码阅读全文

LokiBot 使用新持久化机制和隐写术逃避检测

趋势科技研究人员发现 LokiBot 变种活动通过使用更新的持久化机制和隐写术来隐藏其代码，以逃避检测。攻击始于带有 word 附件的恶意电子邮件，其声称来自印度一家糖果公司。附件嵌入了 Excel 表和标有 'package.json' 的包，执行后将显示 Excel 表，同时执行 VBS 宏，通过调用命令行参数来调用 powershell，然后连接 C2 释放 LokiBot。研究人员通过进一步筛选样本，分析发现 LokiBot 还通过包含恶意 ISO 文件附件的垃圾邮件传播，利用 Windows Installer 进行安装，还使用将恶意代码隐藏在图像中的隐写术来逃避检测。

（原文链接：https://blog.trendmicro.com/trendlabs-security-intelligence/lokibot-gains-new-persistence-mechanism-uses-steganography-to-hide-its-tracks/）

默弗里斯伯勒市水务局网站被伊朗黑客入侵

美国默弗里斯伯勒市水务局账单支付网站遭到伊朗黑客入侵。受攻击网页显示了伊朗国旗和匿名者面具的图片。图片下方信息显示“被伊朗黑客攻击”和“被 Mamad 警告攻击”。该部门立即关闭了网站并启动了内部评估，以确定黑客的来源和受损害程度。默弗里斯伯勒的公共信息官员表示黑客通过旧脚本获得了访问在线门户的权限。由于该网站目前已关闭，客户将无法在线支付账单，该市的 IT 部门正在努力恢复网页并更新安全措施。

（原文链接：https://cyware.com/news/murfreesboro-city-water-departments-bill-payment-website-hacked-by-iranian-hackers-08a8042b）

安全专家披露存在 KDE 软件框架中的 0day 漏洞

安全专家披露存在 KDE 软件框架中的 0day 漏洞，并发布 PoC 代码。KDE Frameworks 是由 KDE 提供的库和软件框架的集合，可用于任何基于 Qt 的软件栈或多个操作系统上的应用程序。

KDE 框架目前被几个 Linux 发行版采用，包括 Kubuntu、OpenMandriva、OpenSUSE 的和 OpenMandriva。该漏洞由 KDesktopFile 类处理 .desktop 或 .directory 文件的方式导致，这些文件允许在受害者的计算机上运行恶意代码。该影响到 KDE framework 包 5.60.0 及以前版本。研究人员没有向 KDE 团队报告该漏洞。

（原文链接：https://securityaffairs.co/wordpress/89527/hacking/kde-zero-day-vulnerability.html）

每周安全事件

类 型	内 容
中文标题	研究人员发布 L0rdix 与 C2 通信时加密方法分析
英文标题	Decrypting L0rdix RAT’s C2
作者及单位	Alex Holland Malware Analyst
内容概述	Bromium 研究人员对 L0rdix RAT 与 C2 通信的加密和解密进行了分析。L0rdix 的配置包含 10 个字段，这些字段被加密，并在 HTTP POST 请求中作为 URL 查询字符串发送到面板的 connect.php 页面。通过从面板发送类似的 POST 请求，可以更新已部署的配置。L0rdix 加密其 C2 通信，首先使用 AES 以密码块链接 (CBC) 模式加密明文，使用 256 位密钥和 16 字节初始化向量 (IV)，然后 Base64 对密文进行编码，用“~”替换“+”字符，最后 URL 对密文进行编码。研究人员发现很多的 L0rdix 样本使用泄露的一个密钥来加密 C2 通信，该密钥可能为默认密钥。
链接地址	https://www.bromium.com/decrypting-l0rdix-rats-c2/

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.Filecoder.a[sys,spr,rog,lck] 2019-08-04	高	该应用程序伪装为色情页面，后台加密手机文件，勒索用户付费解锁，并通过发送短信钓鱼链接进行传播，建议用户立即卸载该应用。
		Trojan/Android.kinkin.c[pay] 2019-08-05	中	该应用程序运行私自调用支付插件，私发订阅短信，监听收件箱短信，拦截并回复，会造成用户资费损耗，请卸载。
		G-Ware/Android.fakeTelegram.d[rmt,exp] 2019-08-06	中	该应用程序伪装成 Telegram 相关应用，接收远程指令，包含打开指定网页、对话框、界面等行为，造成用户资费损耗，建议卸载。
	较为活跃样本	Trojan/Android.TelegramIR.d[prv,exp,sys,rmt,spy]	中	该应用程序伪装系统应用，运行隐藏图标，诱导用户开启辅助服务，窃取通知栏隐私，接收短信指令，修改手机设置，私自进行通话录音，通过回复短信上传位置信息，还会私自进行截屏、上传用户音频文件、联系人、通话记录等隐私，会造成用户隐私泄露和资费损耗，请卸载。
		Trojan/Android.StealMMScreen.b[prv]	中	该应用程序伪装色情应用，运行诱导用户给予悬浮窗权限，跳转微信，后台私自截屏用户微信界面信息、获取用户手机固件信息并联网上传到指定地址，会造成用户隐私泄露，建议立即卸载。
		Trojan/Android.SnowyRat.a[prv,rmt,spy]	中	该应用程序运行隐藏图标，通过 firebase 获取远程指令，上传用户通讯录，短信，照片，录像，音频文件，社交应用信息等隐私信息至服务器，还会根据指令删除用户程序，私发短信，造成用户隐私泄露和资费消耗，请立即卸载。
		RiskWare/Android.9haobocai.a[rog]	中	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。
		RiskWare/Android.ludashiboost.a[exp]	低	该应用程序包含鲁大师手机加速框架，运行后会要求填写注册码，联网下载 WhatsApp，加载广告，存在一定流量消耗，请谨慎使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	NET Framework 远程代码执行漏洞 (CVE-2019-1113)	高	当 .NET Framework 软件无法检查文件的源标记时，会触发远程执行代码漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，那么攻击者就可以控制受影响的系统。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[PSW]/Win32.Kates	中	此威胁是一种专门窃取密码信息的木马家族。该家族运行在 win32 位平台下。该家族感染后会后台连接到远程服务器，将浏览器中的用户账号密码上传。
		RiskWare[PSWTool]/Win32.MailPassView	中	此威胁是一种专门窃取用户密码的风险软件家族。该家族从被感染的计算机中收集窃取密码信息，利用感染者计算机攻击其他电子邮件账户。
		Trojan[Exploit]/SWF.Agent	中	此威胁是一种基于 SWF 格式文件的传播、可以利用漏洞下载恶意代码的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，将大量基因片段定性的恶意代码归类。
		GrayWare[AdWare]/NSIS.Vopak	中	此威胁是一种有广告行为的灰色软件类程序。该家族样本使用 NSIS 打包，NSIS（Nullsoft Scriptable Install System）是一个开源的 Windows 系统下安装程序制作程序。该家族样本通过 NSIS 打包可以捆绑其他恶意代码到用户系统中。该家族运行在 32 位平台下。该家族有安装捆绑软件、修改浏览器主页和修改默认搜索引擎等行为。
		Trojan[DDoS]/Win32.Macri	低	此威胁是一种可以进行 DDoS 攻击的的木马家族。该家族会删除计算机上的安全防护软件，收集并回传计算机信息。

采用硬件方法来防止数据中心内的横向移动攻击

Scott Schweitzer/ 文 安天技术公益翻译组 / 译

IT 部门往往主要关注源自企业外部的网络攻击，即“纵向”攻击。这导致企业容易被危险的攻击者盯上，这些攻击者使用网络钓鱼、恶意软件或“点击诱饵”等手段访问企业的台式机、笔记本电脑等端点。

然后，攻击者将受感染的端点作为据点，在整个企业的服务器中“横向移动”。这种横向移动攻击已经导致了全球多起非常严重的数据泄露事件，引发了广泛关注。

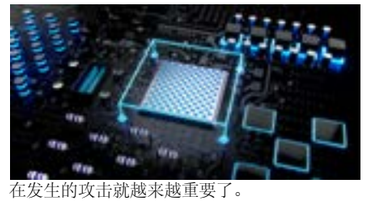
横向移动攻击通常难以检测，而且一旦启动就极难阻止。现在，有一种新方法可以对抗此类攻击，即使用集成网络保护解决方案，这种方法能够创建新的纵深防御硬件安全层。

这种新的安全层能够将每台服务器的硬件防火墙绑定到中央控制器，实现应用程序级的网络分段，以检测、分类和减轻威胁。与目前基于软件的解决方案不同，这种方法在提供保护的同时，不会降低系统性能或增加额外的攻击面，这一点很重要。

横向移动攻击的特殊危险性

服务器之间传输的网络流量越来越容易遭受攻击。网络犯罪分子首先在数据中心内部找到一个入口点，然后将其作为据点，对内部服务器发起横向移动攻击。

据估计，到 2021 年，数据中心内部及各个数据中心彼此之间的横向流量将占数据中心总流量的 85%。横向移动攻击通常是从有效的内部平台发起的。攻击者经常使用劫持的凭证，因此很难将其与受信用户区分开来。当这些受信用户的权限提升（这种事情经常发生）后，使用其凭证的攻击者几乎能够永久性地擦除任何审计痕迹。鉴于此原因，及时检测到正在发生的攻击就越来越重要了。



改善经过验证的防御方法

数据中心管理员尝试使用应用程序级网络分段来对抗横向移动攻击，他们对所有应用程序设置边界和告警，以进行威胁检测、分类和缓解。这些解决方案的问题在于，它们是在软件中实现的，需要超过 15000 个 x86 CPU 时钟周期来过滤每个进站网络数据包。此外，基于软件的应用程序级网络分段为黑客提供了软件攻击面。高明的黑客可以轻松禁用典型的基于操作系统的防火墙。

通过扩展的纵深防御硬件方法，能够消除基于软件的应用程序级网络分段的漏洞，还能提高系统性能。目前的集成网络保护解决方案是：将内置的硬件防火墙与中心化的安全策略管理功能相结合。

这些解决方案可以完成收集、传输和处理数据流的所有工作，而且不会占用任何 CPU 时钟周期。它们的速度比任何防火墙设备都要快 10 倍，但最多产生 200 到 700 纳秒（ns）的延迟。它们的分布式硬件架构本身也具有高容量和无限可扩展性。与传统防火墙不同，它们不会在数据中心网络中形成数据阻塞点，不会导致应用程序的运行速度减慢。

这种纵深防御的硬件方法本身更安全。集成网络保护解决方案的适配器绑定到其 C&C 机制。当它开始报告新的应用程序流时，可以根据这些数据流创建新的安全策略，而这些策略又可分解为单独的防火墙规则。所有操作都会受到服务器自身的防篡改 NIC 平台的保护。（译者注：NIC，Network Interface Card，网络接口卡，简称网卡，也叫网络适配器。）

建立远程控制后，用于查看和管理 NIC 硬件过滤表的本地控制面板将被拆除，这样就无法本地修改板载过滤表了。即使攻击者可以将其权限提升为超级用户或管理员级别，也无济于事，因为访问服务器过滤表的本地路径已被物理拆除。如果攻击者试图篡改适配器，适配器将自行禁用并触发告警。

此外，在该方法中，不存在会被攻击者利用的软件攻击面。在加载任何固件之前，都会验证其真实性。即使具有 root 权限的攻击者也无法修改或禁用这些解决方案——他们只能在网络上看到产出端口。该方法可以配置所有服务器连接，这样攻击者就无法获取有用信息来执行攻击了。通过这种方法，整个平台（从主机到所有固件，以及 C&C 框架和适配器）都会受到保护。

数据中心管理员已经了解了应用程序级网络分段的优势。现在，他们可以既拥有这些优势，同时克服基于操作系统的服务器防火墙的安全漏洞和性能损失。

最新的集成网络保护解决方案使用纵深防御硬件方法，来实现应用程序级网络分段，这从根本上强化了已成为新网络边缘的服务器。这种方法将服务器作为一道关键防线，以保护在数据中心内部及各个数据中心彼此之间横向移动的日益增多的网络流量。

原文名称	Prevent lateral attacks inside the data center with a defense-in-depth hardware layer
作者简介	Scott Schweitzer。Scott Schweitzer 是 Solarflare 公司的技术推广人。
原文信息	2019 年 8 月 6 日发布于 Help Net Security。 原文地址 https://www.helpnetsecurity.com/2019/08/06/defense-in-depth-hardware-layer/
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。