安天发布《Zebrocy Tool 变种木马样本分析报告》

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 Zebrocy 变种木马开始活跃。攻击者通过下载远程模板并引诱用户启用模板中的恶意宏代码的方式传播 Zebrocy 变种。

恶意文档会首先从短链接 hxxps:// bitly / 2G8QrgL 中获取远程模板，该模板内包含恶意的宏代码，它可以从远程模板文件中提取 ZIP 并将其保存到名为 driver_pack.zip 的文件中。该压缩包含有一个可执行文件 comsvc.exe，它可以连接远程服务器并获取其有效载荷。Zebrocy 恶意代码会检查正在运行的进程路径，如果样本没有以 comsvc.exe 的形式运行，它会向 google.com 发送一个 HTTP POST 请求以规避启发式检测。恶意代码会获取卷序列号和屏幕截图，并使用 Github 上提供的名为 psutil 的合法库来收集系统的特定信息，如操作系统版本、系统启动时间、系统正常运行时间、系统 GUID 以及运行进程的 ID，最后以特定的数据结构回传给 C2 服务器，如下所示：project=%3C%230%3E4D291F48%3C%23%230%3E%3C%231%3E[存储卷序列号]%3C%23%230%3E%3C%231%3E[收集的系统信息]%3C%23%231%3E%3C%232%3E[JPEG 格式的屏幕截图]%3C%23%232%3E

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、文件来源信息分析鉴定器、数字证书鉴定器、文件元数据分析鉴定器、动态（Win7 x68）鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、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、动态行为鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	93680d34d798a22c618c96dec724517829ec3aad71215213a2dcb1eb190ff9fa
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.23 MB
MD5	602D2901D55C2720F955503456AC2F68
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Win32.GZ
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=07FADB006486953439CE0092651FD7A6

◆ 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

◆ 危险行为

行为描述	危险等级	附加信息	
延时	★★★	Sleeptime	60000
检测虚拟机	★★★★★	Last TickCount	Time: 27489
		Sleep Time	60000
		Next TickCount	Time: 87716

◆ 常见行为

行为描述	危险等级
壳行为填充导入表	★★
获取系统信息（处理器版本、处理器类型等）	★
访问文件尾部	★
获取计算机名	★
疑似桌面控制	★

◆ 进程监控

PID	创建	命令行
1372	target.exe	"c:\445a3e10621c4037842ec8d899fd4caa\share\target.exe"

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
1372-1.dmp	64720b31e07b1fc1b9458fef37a32ad7	N/A	N/A

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 12 月 24 日 (总第 165 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天移动安全与中国信通院泰尔终端实验室达成移动互联网 APP 安全检测合作

随着移动互联网新业务迅猛发展，移动用户的不断增长，为推动移动互联网行业健康有序发展，维护用户知情权和选择权，保护用户消费权益，优化移动互联网应用安全管理，未来 3 年，安天移动安全与中国信通院泰尔终端实验室将在“移动互联网 APP 安全检测”方面开展深度合作。

2018 年 12 月 19 日，安天移动安全与中国信通院泰尔终端实验室合作签约仪式在中国信通院本部举行，安天移动安全副总经理陈家林与中国信通院泰尔终端实验室副主任马鑫作为双方代表签订合作协议，中国信通院副院长、中国泰尔实验室执行主任何桂立参加签约仪式，并对相关企业加入合作计划表示欢迎。双方将在移动互联网 APP 安全检测方面加强合作，就移动互联网 APP 安全开展技术研究、测试方法研究和平台建设，共同努力打造健康的移动互联网安全生态。

在移动互联网 APP 安全检测合作中，安天移动安全将配合中国信通院泰尔终端实验室提供安全技术和服务支撑，将领先的安全技术转化为坚实的用户安全价值。安天移动安全积极与产业链各方协作，目前已与芯片硬件、厂商系统层、应用开发者、移动应用渠道等移动产业链各方展开全面合作，8 年威胁对抗经验和 15 亿部终端大数据积累是安天移动安全确保本次合作顺利开展的前提。

安天移动安全曾与中国信通院泰尔终端实验室在“预置应用安全检测”上达成合作，此次在“移动互联网 APP 安全检测”方面的合作，标着着双方在合作互信的基础上，合作范围进一步扩大、合作内容进一步加强，也标志着移动互联网安全生态建设步伐进一步加快。

恶意文档构建器 LCG Kit 被利用开展钓鱼活动

Proofpoint 研究人员发现将恶意文档构建器 LCG 工具包作为组件的网络钓鱼活动。攻击首先分发网络钓鱼邮件，其带有 LCG 制作的武器化文档，然后利用漏洞、恶意宏加载有效载荷的 shellcode，完成恶意软件的安装。LCG 最初于 2018 年 3 月被发现，在 3 月和 9 月底的活动中，分别使用 RTF 文档、Excel 文档作为附件，利用 Microsoft 公式编辑器 CVE-2017-11882 和 VB Script 漏洞 CVE-2018-8174，加载 shellcode，安装 Loki Bot、Agent Tesla。11 月底的活动中，转为使用 word 宏来加载 shellcode，来安装 Loki Bot 窃取程序。活动中 LCG Kit shellcode 结合了多种功能实现高度混淆，包括不同文档样本的 Shellcode 将 LCG 参数存储在不同的寄存器中、使用嵌套的垃圾代码、指令之间的相对跳转来混淆反汇编器、指令替代等。研究人员表示该工具可能已在暗网出售，被各种攻击组织用于分发 Loki Bot, FormBook, Agent Tesla, Remcos, AZORult, Revcode RAT, Quasar RAT 等木马。（来源：https://www.proofpoint.com/us/threat-insight/post/lcg-kit-sophisticated-builder-malicious-microsoft-office-documents）

约 10 万打印机再次遭黑客攻击以宣传频道订阅

在“最多 YouTube 订阅者之争”的活动中，黑客曾在 12 月初劫持了 5 万台打印机，打出传单，要求订阅 PewDiePie 频道。

最近黑客又展开了新的攻击活动，再次敦促用户支持黑客最喜爱的 PewDiePie，并在网上匿名呼吁受害者关注和提高打印机安全。该黑客声称，其可以利用打印机固件中的漏洞，连续循环重新向芯片写入数据，最终导致机器损坏。黑客还表示不仅可以打印，还可以捕获敏感文档，甚至在打印时修改文档。

新攻击已影响到包括英国，美国，阿根廷，西班牙，澳大利亚和智利等国家在内的超过 100,000 台机器。（来源：https://www.bbc.com/news/technology-46552339）

网络钓鱼攻击伪装成未送达的邮件以窃取凭证

研究人员 Xavier Mertens 发现了新的网络钓鱼活动，伪装成未送达的 Office 365 邮件通知，窃取用户登录凭据。页面提示用户单击“再次发送”链接以尝试再次发送电子邮件，然后将被重定向到仿冒合法 Office 365 登录的网络钓鱼站点。链接以 # 号加电子邮件地址结尾，这将导致电子邮件地址在页面中自动填充。用户输入密码时，名为 sendmails ( ) 的 JavaScript 函数会将电子邮件地址和输入的密码发送到 sendx.php 脚本，然后将用户重定向到合法的 Office 365 登录 URL。（来源 ;https://www.bleepingcomputer.com/news/security/phishing-attack-pretends-to-be-a-office-365-non-delivery-email/)

每周安全事件

类 型	内 容
中文标题	2019 年预测：简单 Android 恶意软件时代结束
英文标题	Predictions 2019: "The era of simple Android malware is over"
作者及单位	Hauke Gierow
内容概述	Android 恶意软件将变得越来越复杂：网络犯罪分子将原有恶意软件进行包装，采用更多隐蔽措施以防止被反病毒解决方案发现，并以新形式进行传播；利用新的网络技术和标准；对网上银行的攻击将更有针对性和高损害性；“通用数据保护法规”（GDPR）将会更广泛、更有效地执行；随着安全措施的不断增强，简单的 Android 恶意软件的时代已经结束；5G 手机在 2019 年将不会被广泛应用；网络犯罪分子将继续瞄准加密货币进行挖矿；将出现更多利用社交媒体进行虚假情报宣传的社会工程活动。
链接地址	https://thehackernews.com/2018/12/google-plus-hacking.html

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.FakeBank.t[prv,exp] 2018-12-16	该应用程序伪装成银行类应用，运行后隐藏图标，联网后会上传用户设备信息，监听短信，获取用户短信信息并发送到指定号码，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.CalibarSpy.a[prv,rmt,spy] 2018-12-17	该应用程序是一款间谍程序，运行后隐藏图标，后台接收远程控制命令，窃取用户短信、联系人、通话记录、地理位置等隐私信息并上传，私自拍照、录像、静音、拨打电话。会造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.BrazilBanker.a[prv,exp] 2018-12-18	该应用程序运行后弹出银行相关钓鱼界面，模拟点击获取银行相关信息，并上传至服务器。造成用户隐私泄露和经济损失，建议卸载。（威胁等级高）
	较为活跃的样本	G-Ware/Android.SexPay.f[exp,rog]	该应用程序包含色情内容，推送诱惑性内容诱导用户充值付费，为避免用户财产损失，请使用健康绿色软件。（威胁等级中）
		Trojan/Android.QQspy.eb[prv,fra]	该应用程序伪装 QQ，诱导用户输入 QQ 账号密码信息并将其短信私发至指定号码，造成用户隐私泄露，请立即卸载。（威胁等级中）
		RiskWare/Android.WTbocai.a[rog]	该应用程序运行后访问地下博彩网站，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）
		Tool/Android.FMPHelper.a[sys]	该应用程序是游戏辅助工具，可以通过修改游戏权限使用户在游戏中获得特殊功能，用户需付费购买。请谨慎使用，避免造成财产损失。（威胁等级低）
		Trojan/Android.FakeSagawa.a[prv,spy]	该应用程序伪装正常应用，运行后替换默认短信应用，随后隐藏图标，监听拦截用户短信，联网后可上传用户应用列表、手机号、联系人、短信箱内容、固件版本信息等隐私信息，私自发送短信给通讯录联系人，安装未知风险 apk 文件，会造成用户隐私泄露，严重影响用户手机安全，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	Microsoft Word 安全漏洞（CVE-2018-8539）	当 Microsoft Word 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Word 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.StartSurf	此威胁是一种能够修改主页行为的推广类灰色软件类程序。该病毒家族的样本会修改全部浏览器的快捷方式，并将首页地址指向 istartsurf.com。（威胁等级低）
		GrayWare[AdWare]/Win32.Vopak	此威胁是一种有广告行为的灰色软件类程序。该家族运行在 32 位平台下。具有安装捆绑软件、修改浏览器主页和修改默认搜索引擎等行为。（威胁等级低）
		RiskWare[Downloader]/NSIS.DomaIQ	此威胁是一种具有下载行为的风险软件类程序。该家族通常使用 NSIS（开源 Windows 系统下的程序制作工具）将木马与正常程序捆绑在一起。DomaIQ 是一个安装管理器，可以管理要安装或更新的软件，其中包括工具栏、浏览器加载项、游戏应用程序等。（威胁等级中）
		RiskWare[WebToolbar]/Win32.FirstFloor	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族样本运行后会修改注册表中关于浏览器的数据，弹出病毒作者指定的广告页面，干扰用户的正常工作。它的部分变种拥有远程控制和下载器的功能。（威胁等级中）
		Trojan/MSIL.Tpyn	此威胁是一种使用 MSIL 中间语言编写的木马程序。该家族通常会安装并运行广告件程序，窃取用户信息并回传。（威胁等级中）

2019 年云计算预测：云时代来临

John Edwards / 文 安天技术公益翻译组 / 译

Forrester 公司的一份报告指出，企业必须灵活应对不断变化的云市场和云技术。

云计算已经度过了“以自我为中心的‘青少年时代’”，成为“推动全球数字化转型的‘涡轮增压引擎’“。研究公司 Forrester 在其新报告《2019 年预测：云计算》中做了这个生动形象的比喻。该公司预测，到 2019 年，云计算将步入“更有趣的‘成年阶段’”，为企业应用提供创新性的开发服务，而不仅仅是以往那种廉价的临时服务器资源或存储服务。

大型公有云提供商将继续扩大规模

该报告预测到，在 2019 年，全球最大的公有云提供商将继续扩大规模，而企业支出也将激增。报告指出，全球六大云领导者（阿里巴巴、亚马逊网络服务 [AWS]、谷歌、IBM、微软 Azure 和甲骨文）将继续扩大规模——其服务种类和全球覆盖区域都会扩展。与此同时，全球云计算市场规模，包括云平台、商业服务和“软件即服务”（SaaS），将会超过 2000 亿美元，增幅超过 20%。

Forrester 预测到，这六大公有云提供商几乎没有什么有力的竞争者——只有从中国崛起的阿里巴巴，会为其他几大提供商带来一些压力。Forrester 副总裁兼首席分析师大卫·巴特莱蒂（Dave Bartoletti）表示：“目前，还没有新的云平台提供商有足够的资金来挑战这六大提供商。”

容器、Kubernetes（K8s）和“无服务器”计算将重塑核心应用

Forrester 预计，在 2019 年容器技术将继续快速发展。诸如 eBay、ING、Liberty Mutual、Nordstrom 和 Viasat 等公司，都使用基于 Docker 和 K8s（以及 Envoy 和 Istio）构建的云原生平台，为传统应用注入新的活力。

报告指出：“在云原生开源组件和工具的支持下，各公司将开始推出自己的数字应用平台。这些平台将扩展云服务（包括无服务器和事件驱动的服务），为核心企业应用的现代化奠定基础。”该公司称，明年最热门的趋势是：K8s 将更安全，更易于部署、监控、扩展和升级。报告还指出：“来自 Docker、IBM、Mesosphere、Pivotal、Rancher、Red Hat、VMware 和其他公司的企业级容器平台将会快速发展。”

三种新兴的私有云方法

Forrester 指出，各机构必须选择最适合自己的私有云策略。该公司预计，2019 年将出现更多的私有云架构。报告指出，各机构可以采用以下三种方法：（1）使用 vSphere、以开发人员为中心的工具和软件定义的基础架构，在内部构建私有云架构；（2）使用融合或超融合软件堆栈来定制云环境，以最大限度地减少技术负担；（3）依靠自己的技术团队，使用 OpenStack 在内部构建云基础架构。

更多机构将制定 PaaS 策略

Forrester 预测，各机构都将决定是否采用特定云提供商独有的“平台即服务”（PaaS），或者是否采用“云中立”策略。“有些机构会继续使用某种云服务，同时耐心等待供应商中立的增值服务（例如 Istio、K8s 和 TensorFlow）更加成熟，更容易部署。”该报告称。

基于 SaaS 的行业生态系统将崛起

在 2018 年，SaaS 供应商加大了整合力度，Salesforce 收购 API 管理供应商 MuleSoft 和 Workday 以试图扩展其平台就是很好的例子。Forrester 预测，在 2019 年两种 SaaS 趋势（行业和集成）将会融合，形成基于 SaaS 的行业生态系统。该公司预测：“在形成真正的行业生态系统方面，将会出现新兴的、重要的投资。这些生态系统可以实时连接多家公司，促进这些公司之间的分工协作，有利于行业数据分析。”

炒作焦点

巴特莱蒂指出，在新的一年里，区块链将是最大的炒作焦点。“分布式账本有很好的技术支撑，但我认为，大多数公司有更好的选择——即，使用更成熟的云服务来促进应用和技术的转型。”他说。

虽然一些金融分析师认为，当前炙手可热的美国经济可能会在 2019 年放缓，但是巴托莱蒂并不太担心。“我认为，美国经济放缓几乎不会对云计算带来什么影响，如果有，最多也就是影响一年期的发展。”他指出，“相比来说，美国经济放缓将会对数据中心购买技术硬件和本地软件产生较大的影响，不过这些产品早已受到云的压力了。”

建议

“正在为 2019 年做准备的企业，应该尽快进行软件组合分析。”巴托莱蒂说。“最重要的云策略问题是：你希望或需要云应用的哪些方面变得更好。”他还指出，企业只有先确定自己希望获得哪些更好的效果，然后才能选择云平台、云服务或开发平台。

最后，巴托莱蒂进行了总结：“先选择云策略，然后再选择云平台。”

原文名称	Cloud Computing 2019 - The Cloud Comes of Age
原文作者	John Edwards。John Edwards 是一位资深的商业技术记者
原文信息	2018 年 12 月 10 日发布于 InformationWeek 原文地址 https://www.informationweek.com/cloud/cloud-computing-2019-the-cloud-comes-of-age/d/d-id/1333442
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。