安天周观察

主办：安天　2017 年 10 月 30 日（总第 109 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《坏兔子来袭，安天智甲有效防护》报告

安天在 10 月 24 日关注到“Bad Rabbit”（坏兔子）勒索软件的活动情况，并给与了跟踪分析。截至 26 日晚，包括德国、乌克兰、土耳其在内的欧洲多国基础设施遭受病毒攻击，尚未发现国内大面积感染迹象。虽然目前其全球用户影响弱于魔窟“WannaCry”、伪必加“notPetya”等此前的流行病毒，但依然值得高度关注和警惕。

26 日，安天发布相关报告，对该勒索软件样本及其攻击过程进行了深入分析。攻击者采用入侵新闻媒体和其他网站植入恶意链接的方式，进行该样本的初始扩散。当受害者访问这些网站时，病毒伪装为 Adobe Flash 的更新，将下载链接指向到恶意地址，受害者手动点击下载并运行后，就会被病毒感染。该病毒具有通过预设密码档的 IPC$ 弱口令进行内网传播的能力，对内网用户会带来一定威胁。目前未在样本中发现利用其他漏洞进行横向移动传播的行为。

病毒初始传播投放 + 内网扩散传播，已经成为当前网络黑产犯罪的一种重要组合，这使普通互联网用户、政企内网包括关键基础设施，都面临严峻的关联风险。而此前伪必加“notPetya”事件更开启了伪装成勒索软件对关键基础设施进行破坏的先河，目前尚不能对此事件是否是纯粹的勒索攻击还是以破坏作为目的进行更准确的判断。

针对此次事件，安天建议用户警惕第三方未知来源文件下载安装，对安装文件进行签名检测；排查内网弱口令的主机；在终端安装可靠的主动防护产品。经验证，安天智甲终端防御系统对 Bad Rabbit 能够进行有效检测与防护，即使病毒库不进行升级，Bad Rabbit 进行恶意加密时，安天智甲仍然能够及时发现并进行告警。

扫码二维码获取完整版分析报告

安天获公安部重点实验室项目

近日，信息网络安全公安部重点实验室（公安部第三研究所）对由我司康学斌负责的“DDoS 追踪溯源分析技术研究”项目给予了高度肯定，并与安天签署了信息网络公安部重点实验室开放课题合同书。

该项目是由公安部重点实验室开放基金资助的 A 类研究项目，主要对 DDoS 溯源追踪技术进行分析研究，其中涉及多源大数据网络威胁检测、威胁分析、威胁监控与溯源等各个方面。

该项目运用了安天研发产品“安天 BotmonDDoS 威胁情报”的溯源分析技术，该产品在僵尸网络识别、追踪、监控以及威胁情报综合预警和溯源过程中拥有多项具有自主知识产权的国家技术专利。其基于分布式云服务器、大数据、机器学习技术，可对全球 DDoS 僵尸网络进行自动化监控，及时获取精准的攻击情报，为客户提供及时准确的威胁预警，同时还可以对攻击者控制服务器进行追踪溯源。

肖新光：加快人工智能技术的研发和应用

（第 3 版）

安天炼石发布 WPA2 高危漏洞联合分析报告

近日，欧洲鲁汶大学的博士后安全研究员 MathyVanhoef 披露了无线网络（Wi-Fi）保护协议标准 WPA2 的高危漏洞。该漏洞允许在 Wi-Fi 范围内的攻击者监听计算机和接入点之间的 Wi-Fi 流量。其影响协议本身，且对 WPA 和 WPA2 均有效，因此支持 WPA/WPA2 协议的软件或硬件均受到影响。对于利用该漏洞的攻击被命名为 KRACK。

漏洞披露后，安天与炼石的工程师对该漏洞展开了联合深入分析并发布了分析报告。在报告中对漏洞的利用原理、攻击中 Nonce 重用的密码等进行了深度分析，同时对漏洞的影响及部分供应商的响应情况进行了总结；另外，以 Linux 系统的补丁为例，展示了各补丁的作用原理。

KRACK 漏洞利用主要为针对客户端的攻击。因此，用户的路由器可能不需要更新。对于普通家庭用户，应多关注各终端设备厂商的安全公告，及时更新配置或打补丁，优先更新笔记本电脑和智能手机等客户端。目前使用 WPA2 的大多数家庭和商业无线应用客户端升级相对容易，但对于数百万难以及时更新的 IoT 无线设备，可能造成巨大影响。请大家保持警惕，我们会持续关注相关事件并积极应对。

扫码二维码获取完整版分析报告

每周安全事件

类 型	内 容
中文标题	坏兔子 Ransomware 爆发命中东欧
英文标题	Bad Rabbit Ransomware Outbreak Hits Eastern Europe
作者及单位	CatalinCimpanu；BleepingComputer
内容概述	一个名叫 Bad Rabbit 的新型 ransomware 病毒让许多东欧国家遭受破坏，同时影响到政府机构和私营企业。基于 ESET，Emsisoft 和 Fox-IT 的分析，Bad Rabbit 使用 Mimikatz 从本地计算机的内存中提取凭据，并附带硬编码凭据列表，它尝试通过 SMB 访问同一网络上的服务器和工作站和 WebDAV [1，2，3]。对于 Bad Rabbit，ransomware 是一种所谓的磁盘编码器，类似于 Petya 和 NotPetya。Bad Rabbit 首先加密用户计算机上的文件，然后替换 MBR（主引导记录）。一旦 Bad Rabbit 完成了它的工作，它将重新启动用户的 PC，开机便被引导到自定义 MBR 赎金记录。在六月份的爆发中，赎金票据与 NotPetya 使用的几乎相同。尽管如此，与 NotPetya 几乎没有相似之处。Intezer 称 Bad Rabbit 和 NotPetya 之间只有 13% 的代码重用。
链接地址	https://www.bleepingcomputer.com/news/security/bad-rabbit-ransomware-outbreak-hits-eastern-europe/

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.Flyer.a[prv] 2017-10-23	该应用程序为恶意木马，通过联网完善恶意模块，取得设备权限，访问用户信箱、通话记录、照片及存储文件，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.mimahaya.a[prv,rmt,spy] 2017-10-23	该应用程序为一款间谍应用，运行后使用 POC 方案私自提权，接收远控指令，窃取用户信息并上传。造成用户隐私泄露和手机安全危害，请立即删除。（威胁等级高）
		RiskWare/Android.PJbocai.a[rog] 2017-10-24	该应用程序为博彩类应用，包含大量博彩广告，请注意提示信息，避免上当受骗，造成资费损失。（威胁等级中）
		Trojan/Android.Pimobi.a[prv,spy] 2017-10-24	该应用程序是一款间谍工具，运行后激活设备管理，窃取用户通话录音、位置信息、浏览书签、信箱等隐私信息，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.blackjack.a[prv,exp] 2017-10-24	该应用程序伪装 Instagram，诱骗用户输入 ins 账户密码和拦截短信，发送至指定邮箱，并自动发送短信，造成资费消耗和隐私泄露，请立即卸载。（威胁等级高）
		Trojan/Android.jfSMS.a[pay] 2017-10-26	该应用程序运行私自发送付费短信，拦截特定短信，会造成用户资费损失，建议卸载。（威胁等级低）
		Trojan/Android.kcryspy.a[prv,spy] 2017-10-26	该应用程序伪装 Google 应用市场，运行诱导激活设备管理器，窃取用户短信、通话记录、浏览历史、音频文件、WhatsApp、WeChat 聊天记录等隐私信息，造成用户隐私泄露，请卸载。（威胁等级高）
		Trojan/Android.guernica.a[exp,prv] 2017-10-27	该应用程序伪装其他应用，安装无图标，后台释放恶意子包，hook 用户手机大量系统 API 用于形成 " 沙盒 " 来加载其他软件，使用 ixintui SDK 控制程序启动、注册、点击等相关操作私自下载安装软件，造成用户手机流量大量消耗。（威胁等级高）
	较为活跃的样本	Trojan/Android.Locker.r[rog,sys,prv,lck]	该应用程序运行诱导激活设备管理器，诱导用户输入 QQ 账号密码，可能造成用户隐私泄露，并置顶勒索界面，使用户手机无法正常使用，建议立即卸载。（威胁等级高）
		G-Ware/Android.FakeQQpojie.c[fra,rog]	该应用程序伪装成 QQ 破解应用，运行诱骗用户扫码付费激活，程序本身并无实际功能，可能造成用户资费消耗，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash 任意命令执行漏洞 (CVE - 2017 - 11292)	该漏洞为类型混淆型漏洞，其导致攻击者可以在目标系统上执行远程代码。该漏洞影响了众多系统上的 Flash Player 27.0.0.159。Adobe 在 Flash Player 27.0.0.170 版本中对其进行了修复。
	较为活跃样本	Trojan[Backdoor]/Win32.Thunkan	此威胁是一种后门程序。该家族样本使用了简单的加壳手段隐藏自身的关键字符串，运行后会建立后门，可以从远程服务器下载其他恶意代码并运行，有一定威胁。（威胁等级高）
		Trojan[Banker]/Win32.Banaris	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级高）
		Trojan[Ransom]/Win32.Cryptor	此威胁是一种可以加密用户文件并勒索赎金的木马家族。该家族样本运行后遍历系统磁盘并加密文件，向用户勒索赎金以解密，有一定威胁。（威胁等级低）

加快人工智能技术的研发和应用

■ 安天技术负责人 肖新光

一、安天从自动化到智能化的实践和愿景

毫无疑问，安天非常重视通过引入人工智能（深度学习）的技术和方法来提升我们自身的能力，并最终改善客户价值。

从安天的自身实践来看，我们的体会是：坚持扎实的手动分析处理所形成的知识和经验积累，是人工智能的基本经验；大规模自动化批处理的工程实践所形成的工程体系，是人工智能的基础工程。人工智能，人工智能，若无人工何谈智能；若无自动化何谈智能化。安天是最早把自动化分析和特征提取方法引入恶意代码分析对抗领域的企业团队，我们当时的目标很简单，在我们创业的前几年只有七八个人、五六条枪，我们无法依靠极为有限的工程师资源，处理当时每天上千的样本，所以必须依靠自动化的手段。随着我们的发展，基础引擎团队（哈尔滨）逐渐尝试把深度学习引入到样本分析和检测中；移动安全团队（武研）在人工经验和自动化手段的有效融合方面已经达到了国际先进的水平，在大数据和人工智能方面又做出了有效的尝试；深圳团队也做了一些研究性尝试；在画像和自适应方面，北研也有自己的思考。

何老师是公司内部人工智能技术应用的坚定推动倡导者，他在2016年2月翻译了Cylance的演讲“AI对AV”[1]，提议我们加快在AI领域的工作，后续又陆续翻译了《黑客的神经网络指南》[3]、《谷歌案例深入学习演讲》[4]等。对何老师的建议，应该说，是我们重视不够、坚决性不足，对此值得反思。总体上看，我们闭门造车较多，对学术界成果关注不够，基本都是部门自我演进，但缺少整体战略布局。应该说，我司过去几年在主动拥抱具有战略前景的技术方面，不够积极果断。

从后面我们对于人工智能的实践来看，我们要把这种自发的应用，逐渐纳入到我们的战略布局和路线图中。当前我们正在规划我们的下一代综合支撑业务平台“赛博超脑”，“超脑”这一命名，也代表了我们对我们的下一代平台体系具有更强的自动化、智能化能力的期待。同时，在后台将人工智能的模块渐进锤炼成熟后，将逐渐地向前台产品投入。如果说我们的“赛博超脑”是去制造一个超级“大脑”，那我们的态势感知则要形成客户的安全“大脑”，我们的产品在里面要有一个“小脑”。

二、人工智能的一些思考

人工智能其实是一种公共技术，可以应用于任何具有一定复杂度的领域，从网络安全的角度来看，它是攻防双方的公共地带技术。很多人认为防御只要用了人工智能就会变得如何有效，就会获取压倒性的优势，但实际上，攻击者也会使用人工智能。过去，攻击者加工免杀木马是通过批量加工、手工验证的方法，目前则出现了更为智能的自动化免杀。从这个小例子可以看到，智能化也会使整个攻方的效率大大提升。那么在攻击方效率提升的情况下，防御方更需要积极地应用和引进人工智能，才能带来防御效率和效果的改善，才能有效地遏制攻击方。在人工智能领域，我们一定会有所投入，我们也希望在这个方向正式启动组建之后，在相关方面有技术、有积累、有热爱的同事能够积极发力。

综合来看，人工智能，包括深度学习，之前在国内其实已经有两次“虚热”的情况了，但最后都没有发展起来。从本质上来看，一共有两个原因，第一个瓶颈是算力和存储能力不足，人工智能所需要的计算能力和存储能力对于过去而言是非常奢侈的资源，因此建立不起来；第二个瓶颈是人工智能需要有相应的对象，而这个对象就是大数据，如果没有持续的大数据积累，又怎么去做人工智能。但在当前，这两个障碍都被渐进扫除了。

之前我陪同有关院士去视察我省的大数据使用情况，但是后来我发现，各家的大数据似乎都没有我司的多。由于我们有海量的端点、流量侧的积累、样本的持续分析能力，实际上，我们已经形成了一个支撑人工智能的基础数据资源，随着后续的逐步发展，随着我们算力和存储能力的改善，这些问题将不会成为瓶颈问题。

三、以务实的态度进行相关研发工作

我们重视人工智能，不是因为它流行，不是因为它受追捧，不是因为它可以提升我们的估值，而是为了有效提升我们的能力、降低我们的成本、支撑更强有力的产品和服务。

我想强调一点，我们在这个问题上，不要抱有幼稚的想象，更不要沦为“仿生学”安全的空想家。著名的深度学习专家雅恩·乐昆在记者问他“在深度学习的描述中，你最不喜欢的是哪一种”时，他答道“我最不喜欢的描述是，‘它像大脑一样工作’”，这令我对这位研究者肃然起敬。“仿生学”安全是把安全庸俗化的表现。

目前来看，第一，在非常长的一段时间内，还不能创造像人一样思考的机器能力；第二，人工智能是不能完整替代人的。人工智能可以把人的形式化思考作业和形式化利用经验予以体现，使算力达成某种价值，因此，未来的安全对抗，永远是“人+机器”对抗“人+机器”。作为网络安全的保卫者，人工智能是我们的武器，正如毛泽东同志所讲的“武器是战争的重要因素，但不是决定的因素，决定的因素是人不是物”[5]。

——本文是根据安天技术负责人向参观安天来宾的汇报介绍和新员工培训活动中与新员工的对话内容整理而成的。

参考资料

[1]Stuart McClure：《AI vs. AV – Gorillas and Germans and Gartner, oh my…》
https://blog.cylance.com/ai-vs.-av-gorillas-and-germans-and-gartner-oh-my

[2]《对话深度学习专家雅恩·乐昆：让深度学习摆脱束缚》（发表于《中国计算机学会通讯》2015年04期）

[3]Andrej Karpathy：《Hacker's guide to Neural Networks（黑客的神经网络指南）》
http://karpathy.github.io/neuralnets/

[4]Jeff Dean:《A Sampling of Deep Learning at Google（谷歌案例深入学习演讲）》: http://karpathy.github.io/neuralnets/

[5] 毛泽东：《毛泽东选集·论持久战》

安天发布《利用 VMware 传播的木马样本分析报告》

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注意到一个木马样本，该样本是一个利用了 VMware 的正常程序、通过垃圾邮件进行传播的病毒程序。该木马主要针对银行进行攻击，窃取用户的证书，它还使用了多种反调试技术以逃避研究人员分析及沙箱的检测。

安天 CERT 研究人员对样本进行了分析发现，该木马样本与大多数银行木马相似，都是首先利用垃圾邮件进行传播，原始的垃圾邮件是由葡萄牙语编写，由于针对的是南美等使用葡萄牙语的国家，因此收到垃圾邮件的人容易上当并打开附件。该恶意附件的名称使用相关国家的一种发票名称，是一个 html 文件，这个 html 文件包含一个重定向，双击运行该 html 文件后会被重定向到其他链接，下载一个 JAR 文件，如果用户双击并且机器中安装有 java 执行环境的话，银行木马就会开始安装。首先该 JAR 会连网下载其他的恶意文件，然后执行一个正常的 EXE 文件，是经过 VMware 签名的合法的二进制文件，但是，该合法文件依赖的 DLL 中存在着恶意文件 vmwarebase.dll，这样就可以绕过很多安全设备。该恶意 DLL 的功能是注入和执行 explorer.exe 中 notepad.exe 中的恶意代码，其使用的 API 也加入了 AES 加密进行混淆。木马可以终止 msconfig.exe，regidit.exe，cccleaner.exe 等程序，它会获取窗口名，确认用户是否与攻击目标有关，是否打开了 Ollydbg 这样的反调试软件，而且还使用了强力的加密壳，当受感染的主机执行特定操作时，木马会与 C2 服务器进行通信，其配置存放在名为 i.dk 的一个文本文件中。

安天 CERT 提醒广大网络使用者，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。目前，安天追影产品已经实现了对该银行木马样本的检出。

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：

文件被页面手工提交发现，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据动态行为鉴定器将文件判定为木马程序。

文件名	641a58b667248fc1aec80a0d0e9a515ba43e6ca9a8bdd162edd66e58703f8f98
文件类型	Archive/Phil_Katz.ZIP
大小	7.37 MB
MD5	910050BC1FCEA33836FA2E9978BBEA10
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	动态行为

完整报告地址：https://10.255.16.99/_lk/details.html?hash=910050BC1FCEA33836FA2E9978BBEA10

运行环境

操作系统	内置软件
Windows XP 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	行为描述	危险等级
其他进程写入可疑数据	★★★	注入其他进程	★★★★
延时	★★★		

该文件具有以下行为：查找指定内核模块；创建特定窗体；遍历进程；访问其他进程内存；获取驱动器类型；扫描驱动器类型；查找特定窗体；关机；获取计算机名称；请求加载驱动的权限；获取系统版本；获取主机用户名称；打开自身进程文件；独占打开文件；查找浏览器进程；获取 socket 本地名称；获取系统内存。

常见行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
遍历进程	★	访问其他进程内存	★
获取驱动器类型	★	扫描驱动器类型	★★
查找特定窗体	★	关机	★
获取计算机名称	★	请求加载驱动的权限	★
获取系统版本	★★	获取主机用户名称	★
打开自身进程文件	★	独占打开文件	★
查找浏览器进程	★★	获取 socket 本地名称	★

进程监控

PID：1588	创建：C:\WINDOWS\system32\rundll32.exe
	命 令 行：C:\WINDOWS\system32\rundll32.exe fldrclnr.dll,Wizard_RunDLL
PID：1716	dumprep.exe
	命令行：C:\WINDOWS\system32\dumprep.exe 988 -dm 7 7 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WERe72e.dir00\svchost.exe.mdmp 16325836412030804
……	……