安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 10 月 08 日 (总第 154 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

助力民航网安
安天亮相 2018 民航网络安全年会

以“新时代的民航网络安全”为主题的 2018 年民航网络安全年会于近日在天津举行，年会由中国民航局人事科教司指导、中国民航大学主办。来自行业内外的领导、专家、网络安全从业人员等 500 余人齐聚一堂，聚焦民航网络安全热点问题。作为引领威胁检测与防御能力发展的网络安全国家队，安天参与了本次年会并与民航行业内外各位专家交流国际前沿的网络安全防护理念与技术成果，共商新时代民航网络安全的发展方略。

安天首席技术官进行演讲

在年会主论坛上，安天首席技术官潘宣辰带来题为《敌情想定下的网络安全防御思考》的分享。在分享中，他结合了安天在网络威胁对抗上持续积累的技术成果，尝试用系统思维的视角结合民航领域的网络安全防御实践，对敌情想定进行了完善和具象化的介绍，并对安天推动关键信息基础设施防御的规划思路进行了分享。他表示，网络安全的体系化能力建设是一个由基础结构安全、纵深防御、态势感知与积极防御、威胁情报叠加组成的叠加演进过程。

在“网络安全分析与防护技术”的分论坛上，安天研发副总裁王小丰带来题为《明态势、挫威胁 态势感知在监测预警和应急响应中的应用实践》的分享。他指出，态势感知能力的规划和建设，需要以“全面支撑动态综合的网络安全积极防御体系”为目标，建设“感知威胁”、“理解分析威胁”、“预测下一步攻击”、“联动响应处置”、“协同情报、累积知识”五类关键能力。

安天研发副总裁进行演讲

同时，他介绍了安天在态势感知上的主要研发方向，包括“全面监测和按需采集结合，达成全要素的数据采集和威胁感知能力”，“基于知识和深度分析，达成有效的威胁理解能力”，“通过漏洞、攻击者等多线索分析，达成合理的攻击预测能力”，“联动设备、工具、人员及环境，达成快速的响应联动能力”，“利用情报和生产情报结合，达成情报协同能力”等方面的解决方案和实际应用效果。

安天在威胁检测引擎、主机防护、流量监测、动静态自动化分析、APT 深度分析、大数据安全分析等方面有长期自主研发积累。近年来，安天为多个国家和地方主管部门、行管部门研发实施了监测型态势感知解决方案，效果获得了用户好评。这些工作也同时推动了安天对“高信息价值、高防护等级、高威胁对抗”场景下的网络安全建设规律和解决方案的思考，重新认识了重要信息系统和关键信息基础设施对态势感知和积极防御的安全需求。在监测型态势感知的经验积累下，持续加强对实战型态势感知的研发投入，努力与关键基础设施管理者、行业客户携手共建实战化的态势感知体系，依托全面持续监测能力，逐渐形成分析预测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，推动客户整体安全能力建设的叠加演进。

民航业作为国家交通的基础工具，承担了人们的日常外出和国内物流运输的重要责任，是关键基础设施的一部分，其网络安全直接影响国家安全、社会发展和人民的日常生活。安天近年来已分别在中国民用航空局“民航网络与信息安全管理平台”、中国商飞“C919 大飞机首飞网络安全保障”、中国国际航空公司“信息安全风险评估服务”、首都机场“网络安全综合保障服务”、中国航信“信息系统产品威胁建模服务”等项目中承担了关键角色，并获得了客户的一致好评。通过参加此次民航网络安全年会，安天期望与更多的民航业客户进行深入交流，并以安天自身成立 18 年来不断积累的安全实战能力，为民航行业的网络安全能力体系建设作出贡献。

每周安全事件

类 型	内 容
中文标题	研究人员发现 macOS Mojave 中的隐私绕过漏洞
英文标题	Apple MacOS Mojave zero-day privacy bypass vulnerability revealed
作者及单位	Charlie Osborne
内容概述	Apple Mojave发布当日，研究人员指出其存在隐私绕过漏洞。研究人员提供了一分钟视频显示了如何破坏Mac操作系统，绕过隐私控制并允许访问用户敏感数据（如地址簿中信息），并表示零日漏洞源于Apple实施各种隐私相关数据保护的方式。 macOS Mojave为保护用户数据，要求用户授权应用访问位置服务、联系人、日历、提醒、照片以及其他私人信息和文件，但攻击者可以使用没有任何特权的应用来利用零日漏洞。
链接地址	https://www.zdnet.com/article/macos-mojave-zero-day-privacy-bypass-bug-revealed-on-the-day-of-download/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有9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.netSecurity.a[prv,rmt,exp,spy] 2018-09-25	该应用程序伪装为系统应用，运行后隐藏图标，接收远程控制指令，上传用户短信、通话记录、文件列表、QQ、微信、Facebook的相关隐私信息，还会在后台进行拍照、录音、控制手机振动、删除文件、发送短信、拨打电话等操作，造成用户隐私泄露和资源消耗，建议立即卸载。（威胁等级高）
		Tool/Android.PhoneSpector.a[prv,rmt] 2018-09-25	该应用程序是一个付费手机监控应用，在取得授权码之后可以获取用户的短信信息、通话记录、联系人、浏览器历史、图片、视频、Facebook消息等，并把信息上传到指定网址，通过登录账户可以查看受控手机的上传内容，建议谨慎使用，若非自主安装建议卸载。（威胁等级中）
		Tool/Android.CommAssist.a[prv] 2018-09-26	该应用程序是一款防盗应用，会上传用户联系人、通话记录、短信到用户设置的指定邮箱，造成用户隐私泄露，请谨慎使用。（威胁等级中）
		Trojan/Android.PrismBackDoor.a[prv,bkd] 2018-09-27	该应用程序的elf文件中包含反弹shell，恶意攻击者会通过后门对用户造成安全威胁，建议用户立即卸载。（威胁等级中）
		G-Ware/Android.ResetPW.a[rog,sys] 2018-09-28	该应用程序运行诱导激活设备管理器，而后锁屏，并重置锁屏密码，影响用户手机的正常使用，建议卸载。（威胁等级中）
	较为活跃的样本	Tool/Android.bombcall.e[exp]	该应用程序运行后访问电话轰炸类网站，需要付费使用，可能影响他人手机的正常使用，建议谨慎使用。（威胁等级低）
		Trojan/Android.Terbod.e[prv]	该应用程序伪装正常应用，运行后隐藏图标，利用Telegram提供的通讯接口，窃取用户通讯录并联网上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.TrackerSpy.b[prv,spy]	该应用程序伪装系统应用，实际是间谍件，通过设置、隐藏图标、后台上传用户通话记录、联系人、程序安装列表、收件箱信息等隐私信息，建议立即卸载。（威胁等级中）
		Trojan/Android.Bahamut.c[prv,spy]	该应用程序伪装为正常应用，内嵌恶意代码，运行会上传手机相关信息、用户邮箱信息、文件信息、联系人信息等，并能够监听电话拨号，私自录音，造成用户隐私泄露，建议卸载。（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 Excel 远程代码执行漏洞（CVE-2018-8331）	当Microsoft Excel软件无法正确处理内存中的对象时会触发该漏洞。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。
	较为活跃样本	Trojan[Dropper]/Win32.Miner	此威胁是一种可以释放比特币挖矿机的木马家族。该家族样本运行后释放恶意代码到本机并运行，连接网络下载比特币挖矿机，占用系统资源，影响用户使用。（威胁等级高）
		Trojan[Dropper]/Win32.Injector	此威胁是一种带有捆绑行为的木马类程序。该家族会在被感染的电脑中安装被压缩的恶意软件，并为黑客打开后门。该家族通过用户在成人网站或共享网站上下载的编解码器和AcitveX更新来感染电脑。该家族进入系统后隐身运行，并会弹出恶意弹窗。（威胁等级中）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种后门类木马程序。该家族是通过AutoIt编写的后门程序。样本运行后会连接远程服务器，等待接收上传下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。（威胁等级高）
		Trojan[Ransom]/Win32.Spora	此威胁是一个勒索软件家族。该家族的样本在执行后会加密多个类型的文件，并生成一个KEY文件（密钥文件）和一个LST文件（加密过的加密文件列表），在加密后向用户勒索赎金。（威胁等级中）
		Trojan[Dropper]/Win32.Agent	此威胁是一种以基因片段定性的木马类程序。该家族以捆绑安装为主要传播手段，将木马程序与正常软件捆绑，并将捆绑后的文件上传到下载网站中。（威胁等级高）

黑客瞄准房地产交易，或导致可怕的后果

AFP / 文　安天技术公共翻译组 / 译

詹姆斯·布彻（James Butcher）和坎迪斯·布彻（Candace Butcher）夫妇准备购买他们梦寐以求的退休家园，他们根据房地产结算公司发来的电子邮件中的汇款说明，通过银行转账向该公司支付了 27.2 万美元。

然而在几个小时后，他们汇的那些钱却不翼而飞了。

科罗拉多州的布彻夫妇并不知道，该房地产结算公司的电子邮件帐户已被黑客入侵，黑客更改了汇款说明中的收款账户，成功窃取了他们几乎一生的积蓄，州法院提起的诉讼指出。

美国联邦调查局（FBI）互联网犯罪投诉中心（IC3）的一份报告称，2015 年至 2017 年，涉及房地产交易的电子邮件诈骗受害者人数增加了 1110%，损失增加了近 2200%。该报告称，2017 年有近 1 万人上报了此类诈骗案件，受害者的损失超过 5600 万美元。

根据布彻夫妇的律师伊恩·希克斯（Ian Hicks）的说法，布彻夫妇没能搬进他们的梦想家园，而是不得不搬进了他们儿子家的地下室。他们对房地产经纪人、银行和结算公司提起了诉讼，最后达成了秘密协议。

房地产业务链中安全措施的缺失，以及获得巨额回报的潜力，导致该行业的黑客攻击问题日益严重。

希克斯参与了美国十几起类似案件的诉讼，他说：“在这些案件中，诈骗者知道交易的所有细节，甚至是完全保密的内容，他们本不应该知道这些。”

电子邮件并不安全

美国各地的法院立案调查了很多这样的诈骗案件。首都华盛顿特区的一对夫妇称，在一起类似的诈骗中损失了 150 万美元。

房地产行业只是 FBI 所谓的“企业电子邮件攻击”（BEC）诈骗的一部分。在过去的五年中，BEC 诈骗导致了约 120 亿美元的损失。但对于购房者而言，这种诈骗的后果尤其严重。

“在这些案件中，受害者的损失可能是灾难性的，足以颠覆他们的生活。”希克斯说。

房地产交易“涉及大额资金，而且房地产公司的员工不擅长安全技术”，因此攻击该行业的利润非常丰厚，安全公司 Proofpoint 的威胁研究主管谢罗德·德格瑞普（Sherrod DeGrippo）说。此外，黑客经常通过窃取信息来了解交易内容，“有时，他们甚至比房地产公司的员工更了解交易内容。”她说。

德格瑞普指出，如果购房者对新家非常憧憬，就会少些防备心理，因此很容易沦为此类诈骗的受害者。“这些社会工程策略依赖于购房者的兴奋情绪，他们在购买梦想家园时就处于这种情绪中。”她补充道。

德格瑞普表示，这些诈骗者似乎来自海外，可能是俄罗斯或非洲，他们采用各种技术规避执法部门。“他们雇用很多‘钱骡’，”她说，“这些‘钱骡’按照指令，去一家银行的 ATM 机取现，再存到另一家银行，如此往复。”

美国银行家协会（American Bankers Association）风险和网络安全高级副总裁保罗·本达（Paul Benda）表示，银行一直在努力应对日益严重的诈骗问题，但往往无法阻止电子邮件帐户被黑导致的诈骗。“银行拥有非常强大的安全控制措施，”他说，“但是，当他们接到客户的汇款要求时，他们有责任将钱款汇到指定的账户。”本达指出，客户需要知道，汇款“就像现金一样”，可能无法追回，特别是如果它最终被汇到了海外。

谁应该负责？

购房者的起诉对象通常是房地产经纪人、律师、托管代理人、银行和准备交易文件的结算公司。

美国房地产经纪人协会（National Association of Realtors）高级顾问芬利·马克森（Finley Maxson）说：“房地产交易涉及各方人员，诈骗者可以攻击他们之中的任何一个。”

“诈骗邮件变得更加高明，更难以捕获。”马克森表示，房地产经纪人协会和其他协会正在积极地向相关各方普及诈骗知识，敦促他们采取更好的安全措施。“我们警告他们，不要通过电子邮件发送汇款说明。”他说。在多方参与的情况下，可能很难确定责任方。但是希克斯指出，“购房者不会对他们一生的积蓄掉以轻心”，房地产经纪人有责任确保他们的电子邮件安全，并为客户提供充足的信息。

希克斯为布彻夫妇提起的诉讼称，“在房地产行业中，布彻夫妇遭遇的骗局并不新鲜，本可以很容易地预防。”

今年初，堪萨斯州的一家法院对一起类似案件进行了判决，一名电子邮件帐户被黑客入侵的房地产经纪人被判承担 85% 的责任，赔偿购房者 167,129 美元。

希克斯表示，在这些案件中，“相关各方都可以逃避责任。除非房地产公司和结算公司需要赔偿购房者的损失，否则他们不会采取必要的安全措施来保护购房者的权益。”

原文名称	Hackers Target Real Estate Deals, With Devastating Impact
原文作者	AFP
原文信息	2018 年 9 月 23 日发布于 SecurityWeek 原文地址 https://www.securityweek.com/hackers-target-real-estate-deals-devastating-impact

安天发布《GandCrab V5 勒索木马分析报告》

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GandCrab勒索木马已经出现了第五个版本，GandCrab V5。其拥有一些明显的变化，最明显的就是它使用了5个随机字符作为加密文件的扩展名并且增加了html格式的勒索信息。

研究人员发现，GandCrab V5勒索软件目前正通过广告件进行传播，样本运行后会重定向到带有Fallout漏洞利用工具包的网站。由于漏洞利用工具包利用访问者系统中的漏洞来安装恶意代码，受害者将在不知情的情况下被感染，直到他们发现加密文件和勒索信息为止。

GandCrab V5运行后，将扫描计算机和任何网络共享文件进行加密。扫描网络共享时，它会枚举网络上的所有共享，而不仅仅是映射的驱动器。当遇到目标文件时，它将加密文件，然后附加一个随机的5个字符的扩展名。在加密文件时，勒索软件还会创建名为[extension] -DECRYPT.html和[EXTENSION] -DECRYPT.txt的勒索信息，其中包括文件加密的说明以及如何访问Tor网站以支付赎金的说明，该域名为http://gandcrabmfe6mnef.onion。受害者通过链接访问Tor网站后，会显示赎金金额以及如何支付以获取解密工具的说明。目前勒索金额为价值800美元的达世币（DASH）。

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。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、文件来源信息分析鉴定器、数字证书鉴定器、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	d77378dcc42b912e514d3bd4466cdda050dda9b57799a6c97f70e8489dd8c8d0
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	183 KB
MD5	07FADB006486953439CE0092651FD7A6
病毒类型	木马程序
恶意判定/病毒名称	Trojan/Win32.Ransom
判定依据	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
Windows 7 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	附加信息	
查找游戏进程	★★★★	string1	steam.exe
疑似查找游戏进程	★★★★	steam.exe[steam]	steam.exe[steam]

常见行为

行为描述	危险等级
遍历进程	★
获取计算机名称	★
查找反病毒程序	★★
获取驱动器类型	★
获取系统内存	★★
连接特殊URL	★
获取CPU信息	★★
疑似查找杀软进程	★★
扫描驱动器类型	★★

文件扫描

文件名	文件MD5	家族相似性	
target.exe	07fadb006486953439ce0092651fd7a6	N/A	N/A
target.exe.dmp	437e4649f8edbeb8a4ad6e50456ca6b9	N/A	N/A
index.dat	9069ca035c19a71d375ce667e007ce86	N/A	N/A