安天发布《Ursnif银行木马变种分析报告》

近日，安天CERT在梳理网络安全事件时发现一个名为Ursnif的银行木马变种程序。Ursnif又名Dreambot，Gozi和ISFB，多年来一直活跃在境外，此次Ursnif银行木马在国内爆发，主要借助Pushdo钓鱼邮件僵尸网络进行传播。Pushdo钓鱼邮件僵尸网络，是由数量庞大的计算机构成的能够自动对外发送钓鱼邮件的网络。攻击者将已感染的机器变为垃圾邮件分销点，以此控制更多的机器。

该钓鱼邮件以伪装成极具诱惑性的DHL快递单为诱饵，诱使用户打开附件中的Excel文档。该Excel文档中包含恶意宏代码，用户一旦启用宏，钓鱼文档就开始向计算机释放Ursnif银行木马和Pushdo钓鱼邮件投递器。Ursnif银行木马执行后，使用了反调试技术使其难以分析。例如，该木马隐藏了一些API函数，每次调用这些函数时都会动态解析，因此静态分析十分困难。并且主模块中的大多数数据都是加密的，只有在运行时才会解密。在进行进程分析时，会有非常多的“iexplorer.exe”进程启动和结束，并且发现该进程中有流量进行传输。主要原因是该木马使用COM实例将数据发送到C&C。用户电脑中存储的银行账户，浏览器凭证等敏感信息都将被窃取。

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。

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、关联分析鉴定器、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、来源信息鉴定器、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、关联分析鉴定器、反病毒引擎鉴定器、信标检测鉴定器将文件判定为木马程序。

◆概要信息

文件名	aac9d2d21f634157eb8d3867a2c72042a83cabc3f0142b12763312f5a0b0a83a
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	296 KB
MD5	59CEADA6218D87ED00FEE4D025AE58C7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/Win32.Ursnif
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=59CEADA6218D87ED00FEE4D025AE58C7

◆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
检测虚拟机	★★★★
延时	★★★

◆常见行为

行为描述	危险等级
加载运行时DLL	★
获取系统信息(处理器版本、处理器类型等)	★
壳行为填充导入表	★★
获取计算机名	★

◆常见行为

源IP	源端口	目的IP	目的端口
192.168.122.165	61371	192.168.122.1	53
192.168.122.165	53952	192.168.122.1	53
192.168.122.165	65262	192.168.122.1	53
192.168.122.165	55700	192.168.122.1	53
.....	.....	.....	.....

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19日(总第196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 安天力推实战化威胁猎杀

以“坚守网络空间 护航民航强国”为主题的2019民航网络安全年会于8月8日至9日在哈尔滨举行，年会由中国民用航空局人事科教司指导、中国民航大学主办、民航东北地区管理局协办。来自行业内外的领导、专家、网络安全从业人员等300余人齐聚一堂，交流分享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，安天在大会报告环节力推实战化威胁猎杀服务。

安天技术负责人解读威胁猎杀

年会上，安天带来了题为《实战化威胁猎杀，让威胁无所遁形》的报告，强调了在“敌已在内、敌情不明”的严峻形势下开展威胁猎杀工作的必须性；解读了威胁猎杀的定义与要素，详细介绍了安天正在规划完善的威胁猎杀服务的整体运行流程，并总结了安天此前在与方程式、海莲花等高级网空威胁行为体隔空对决的经验教训。

微信扫描二维码阅读全文

安天发布微软远程桌面服务RCE漏洞预警

微软发布了八月份补丁更新，修复漏洞中包含远程桌面服务中的远程代码执行（RCE）漏洞，漏洞ID为CVE-2019-1181和CVE-2019-1182。这两个漏洞与之前修复的“BlueKeep”漏洞（CVE-2019-0708）一样，攻击者利用漏洞无需用户的交互，即可实施攻击，可用于传播类似“WannaCry”（魔窟）的蠕虫病毒。受影响的Windows版本是Windows 7 SP1、Windows Server 2008 R2 SP1、Windows Server 2012、Windows 8.1、Windows Server 2012 R2以及所有受支持的Windows 10版本，包括服务器版本。目前还未发现该漏洞被第三方利用。安天智甲可以帮助用户检测是否受漏洞影响，并安装补丁程序修复漏洞。

（原文链接：https://mp.weixin.qq.com/s/OWMdIEMoWUMDdygEB8kpgQ）

新版本PsiXBot使用短链接搜索DNS服务器

Proofpoint研究人员发现新版PsiXBot恶意软件的攻击活动。新版PsiXBot检查受感染机器的安装语言，如果是俄语将退出，使用短链接收集每个C&C域的当前DNS服务器，具体过程为：首先对要使用的DNS服务器的十六进制编码的IP地址的非预期GET请求；Ping到DNS服务器IP地址以获取连接状态；对.bit域的DNS查询，返回C & C IP地址；Ping到C & C IP地址以获取连接状态；最后收集到C & C域的HTTPS流量。新版本PsiXBot还包含多个新模块，可实现删除正在运行的僵尸网络进程、监视剪贴板中加密货币钱包地址并窃取、表单抓取、使用Microsoft Outlook发送出站电子邮件等功能。

（原文链接：https://www.proofpoint.com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure）

英国航空公司登机系统漏洞暴露乘客数据

Wandera研究人员调查发现英国航空公司办理登机手续系统存在安全漏洞，可允许能够访问客户网络数据的黑客收集乘客个人身份信息。研究人员发现英国航空公司通过电子邮件向客户发送登录其航班的链接时，该消息通常通过中间服务器发送。该链接包含乘客姓氏和预订信息等数据，旨在帮助收件人自动登录其帐户。但由于URL未加密，拦截链接的外人可以使用姓氏和预订数据来获取有关乘客的更多信息。研究人员没有提供有关此漏洞被利用的证据。

（原文链接：https://www.wandera.com/mobile-security/british-airways-vulnerability/）

被泄露的StockX数据库正在线销售和传播

上周StockX遭到黑客入侵，攻击者窃取了用户帐户信息。目前研究人员发现包含684,0339个用户帐户的StockX数据库正在网上销售和分发，StockX数据库最初是以300美元的价格在Apollon出售，后来变为用户名和密码组合以2.15美元在暗网出售。被泄露的信息包括用户名电子邮件地址、地址、鞋号、购买历史记录和加密密码。黑客表示已经开始解密密码，这些账户凭据可能被用于未来的攻击。

（原文链接：https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/）

每周安全事件

类 型	内 容
中文标题	网络钓鱼活动伪装成异常登录的微软警报
英文标题	Beware of Fake Microsoft Account Unusual Sign-in Activity Emails
作者及单位	Lawrence Abrams
内容概述	研究人员发现了伪装成“异常登录活动”的微软警报的网络钓鱼活动。攻击者通过发送假冒微软向用户发送“Microsoft 帐户异常登录活动”的警报钓鱼邮件，邮件中带有“查看最近活动”电子邮件链接。由于谷歌和微软等公司通常会在用户帐户中发现异常活动时向用户发送警报，所以用户可能会认为收到的是正常通知。点击链接后，将被带到虚假的微软账户登录页面，当受害者输入凭证时，这些信息将被保存起来供攻击者稍后检索，窃取凭据。
链接地址	https://www.bleepingcomputer.com/news/security/beware-of-fake-microsoft-account-unusual-sign-in-activity-emails/

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 平台的恶意代码和漏洞值得关注

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.DownAnubis.c[exp,rog] 2019-08-11	高	该应用程序伪装为知名应用，运行以安装 GooleService 的名义加载银行木马，造成用户的资费消耗和隐私泄露，存在较大的安全风险，建议卸载。
		RiskWare/Android.AdFraudClick.a[exp,rog] 2019-08-12	中	该应用程序为游戏应用，捆绑广告件，运行推广 Happy Bay 游戏平台，诱导用户使用，可能造成用户的资费消耗，建议谨慎使用。
		Trojan/Android.Asacub.f[exp,rog] 2019-08-13	中	该应用程序内嵌恶意代码，运行动态加载恶意子包反射调用，警惕该程序私自窃取用户隐私信息，建议卸载。
	较为活跃样本	Trojan/Android.nbank.l[prv,rmt,spy]	中	该应用程序为间谍件，私自禁用或卸载指定应用，接收指令，上传用户联系人、短信、通话记录等隐私，还会私自拨打电话，修改通话记录，会造成用户隐私泄露，请卸载。
		RiskWare/Android.Dabaoji.a[rog]	中	该应用程序通过打包机生产，运行访问第三方网贷、博彩、网赚等地址，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。
		Trojan/Android.SmsSpy.ca[prv,rog]	中	该应用程序伪装安全助手，无实际功能，运行诱导用户开启辅助服务、隐藏用户短信通知，后台上传用户短信，造成用户隐私泄露，请立即卸载。
		Trojan/Android.FakeWallet.d[fra]	中	该应用程序伪装电子货币钱包，运行后诱导用户输入账号密码，可能会窃取用户电子货币钱包账号和电子货币，给用户带来经济损失，建议立即卸载。
		G-Ware/Android.ResetPW.b[sys]	低	该应用程序包含风险代码，诱导激活设备管理器后，私自重置密码，影响用户正常使用，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft SQL Server 远程代码执行漏洞（CVE-2019-1068）	高	微软 SQL 服务器不正确地处理内部函数时会触发远程代码执行漏洞。成功利用该漏洞的攻击者能够在 SQL 服务器数据库引擎服务账户中执行代码。要利用该漏洞，认证后的攻击者需要向受影响的 SQL 服务器提交一个特殊构造的查询请求。
	较为活跃样本	Trojan/Win32.Addrop	中	此威胁是一种具有下载行为的木马家族。该家族样本感染计算机后会在计算机上生成文件、更改注册表、将自身代码注入到其他程序中。该家族木马会链接远程服务器下载恶意软件到感染者计算机中。收集计算机信息并回传。
		Trojan[Monitor]/Win32.WebWatcher	中	此威胁是一种具有监听功能的木马程序。该家族样本通过频繁快照监控记录用户，并将收集到的图片信息回传到指定的电子邮件。
		GrayWare[AdWare]/Win32.FlyStudio	低	此威胁是一种具有广告件行为的灰色软件家族。它将恶意代码注入系统中并执行。它还会在 Windows 文件夹里面创建一些可执行文件。此外它还会修改，并创建注册表项，在 Windows 启动时自动运行，向感染者电脑中弹出广告。
		GrayWare/MSIL.DomaIQ	低	此威胁是一种具有广告件行为的灰色软件家族。该家族样本使用 MSIL 语言编写。DomaIQ 是一个安装管理器，它可以管理你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。该家族会在感染者计算机中弹窗推送广告。
		HackTool[Hoax]/Win32.FakeInstaller	低	此威胁是一种恶作剧类木马程序。该病毒家族伪装成下载器，运行后向用户发布虚假消息。

弥补网络风险与业务风险之间的差距

Josh Lefkowitz/ 文 安天技术公益翻译组 / 译

对网络风险和业务风险之间认识的不一致，是企业首席信息安全官（CISO）、高管和董事会之间无法达成一致的最大原因和表现。其中一个问题在于，目前用于衡量和管理业务风险的许多流程和工具早在网络风险（或者说网络）出现之前就已建立了。更糟糕的是，各种安全工具的功能之间往往是孤立的，它们的很多功能无法扩展到业务领域（更不用说业务风险领域了）——同样的，业务领域的流程和工具也难以扩展到网络领域。

但是，无论无法达成一致的原因是什么，这种不一致都会带来问题。正如我在前一篇专栏文章中所述，业务风险是指企业因不确定性而遭受损失的可能性，这包括与网络基础设施相关的不确定性。换句话说，业务风险与网络风险并不是相互独立的——业务风险包含网络风险。这也意味着，企业只有在考虑网络风险，并将其与业务风险保持一致时，才能有效地管理业务风险。

以下是帮助 CISO 和其他安全从业者实现这种一致性的几个建议。

用管理层能听得懂的话来讲网络安全风险

没有安全背景的企业领导者不熟悉安全术语，其中一些领导者甚至不了解安全会如何影响业务和业务风险。

举例来说，CISO 会如何将未打补丁的漏洞所带来的风险传达给其管理团队呢？他们可能会这样说：

“虽然该漏洞还未被广泛利用，但它存在于关键系统中，会导致远程代码执行，并且存在概念验证（POC）漏洞利用代码。因此，必须将其列为高优先级漏洞并立即打补丁。”

但是，CISO 可以调整一下说法，以便更好地与业务领域的受众（如高管）产生共鸣。例如，他们可以这样说：

“此漏洞对客户数据的机密性构成重大风险。我们应立即修复漏洞来消除此风险。如果不修复漏洞，我们将不得不面对这种漏洞被利用导致的业务风险。如果客户数据因此受到损害，公司很可能会面临声誉损失、客户忠诚度侵蚀和监管违规等问题，从而遭受重大经济损失。”

量化风险

网络风险的另一个独特挑战是：难以量化。其他类型的业务风险（从诈骗和合规风险到信用和运营风险），可以，并且通常，与风险评估和管理过程中的业务损失相关联。事实上，这个过程通常是，高管和董事会跨业务职能分配预算和资源的过程。但是，虽然企业很容易评估新的反诈骗控制措施能够减少的诈骗损失，但是对于网络风险和为管理它们而实施的控制措施来说，这种评估并不容易。

网络安全中存在更多未知威胁，但是可以帮助风险分析师和安全从业者准确估计这些未知威胁的历史数据却要少得多。因此，CISO 致力于寻找可用的历史数据以及威胁情报——更具体地说，是业务风险情报（BRI），以便更好地了解和预测企业最容易遭受的风险。风险评估框架也是一种有用的资源。某些较新的框架，如 FAIR 框架，旨在帮助企业更准确地量化风险。

制定“风险偏好”

企业为实现其业务目标而能承受的风险被称为“风险偏好”（ risk appetite）。许多企业通过风险偏好声明阐明了其风险偏好。风险偏好声明是一份简明扼要的文件，概述了企业在其运营背景和环境中将会和不会容忍的风险类型和数量，以及原因。以下是风险偏好声明的一个例子：

作为一家大型零售商，我们在追求收入目标、提高运营效率和培养客户忠诚度方面面临一系列风险。要想实现这些目标，需要承受一些风险。我们对可能危及关键资产（包括知识产权、敏感数据和人员）的风险具有低偏好—即不能接受；对声誉风险具有中等偏好—即可以接受；对市场竞争或创新所带来的战略风险则具有高偏好—即可以接受这种风险。我们尽力将所有风险控制在可接受的水平或低于可接受的水平。

然而，许多企业要么没有创建风险偏好声明，要么风险偏好声明是没有 CISO 参与的情况下发布的。

如果企业尚未创建风险偏好声明，CISO 可以与适当的利益相关方（通常包括其他高管、董事会和其他高级领导者）合作，在考虑网络风险的情况下创建一份风险偏好声明。如果企业已经在未考虑网络风险的情况下创建了一份声明，那么 CISO 可以创建一个独立的、与前声明互补的声明，以便与业务目标保持一致。

在这两种情况下，最重要的是将企业的网络风险、网络风险控制措施和支持数据置于企业背景中，以便与整个企业的利益相关者和决策者产生共鸣

原文名称	Tips for Bridging the Gap Between Cyber Risk & Business Risk
作者简介	Josh Lefkowitz。Josh Lefkowitz 是 Flashpoint 公司的首席执行官。
原文信息	2019 年 8 月 12 日发布于 Security Week。 原文地址 https://www.securityweek.com/tips-bridging-gap-between-cyber-risk-business-risk
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。