安天发布《DanaBot 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 DanaBot 的木马变种程序，该木马程序通过钓鱼邮件进行传播。DanaBot 木马主要在澳大利亚、新西兰、美国和加拿大等国家传播，最近已经蔓延至欧洲。该钓鱼邮件以核对收费账单为诱饵，诱使用户打开附件中的 word 并点击文档中的链接。用户点击该链接后会下载一个 VBS 脚本，该脚本运行后会在 %TEMP% 目录下释放 DanaBot 下载器并将其注册为服务。

DanaBot 木马新变种中加入了勒索模块，该模块是用 Delphi 编写的名为 crypt.exe 的勒索软件。crypt.exe 执行后会在 %TEMP% 目录下释放一个名为 b.bat 的批处理文件，b.bat 文件主要功能是停止进程、停止服务以及删除卷影副本等。用户一旦感染 crypt.exe，会导致系统除 Windows 目录外的所有文件被加密。该勒索软件使用 AES128 算法加密文件，文件加密后会被追加扩展名 .non。crypt.exe 创建名为 HowToBackFiles.txt 的勒索信，每 14 分钟创建一次加密任务。安天 CERT 分析人员通过关联分析发现 DanaBot 木马新变种中的勒索模块是 Blitzkrieg 勒索软件的变种。国外研究员 Yaroslav Harakhavik 和 Aliaksandr Chailytko 已经开发出了 Blitzkrieg 勒索软件的解密工具。此外 DanaBot 木马还具有以下功能：通过 RDP 或 VNC 提供远程控制、通过 TOR 匿名网络请求更新、利用 WUSA 漏洞绕过 Windows 用户账户控制（UAC）和从 C&C 服务器请求更新或执行命令等。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；收发邮件时要确认收发来源是否可靠，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采取 VPN 连接等安全方式，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、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、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	8a21e1224a8f1d7dd9d4e42c78c829fb82808631577477e8f699f15feb7c8988
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	144 KB
MD5	E48067D2AD6ADCBF2E4CF7E705D4BD82
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.CryFile
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=E48067D2AD6ADCBF2E4CF7E705D4BD82

◆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
创建可疑进程	★★★★
文件篡改	★★★★★
执行解释型脚本	★★★
移动启动目录，疑似突破主动防御监控自启动目录	★★★
攻击杀软之关闭进程	★★★★
USP 进行劫持	★★★
dll 劫持	★★★★★

◆常见行为

行为描述	危险等级
连接网络	★
创建挂起进程	★★
获取驱动器类型	★
自我复制	★★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
设置自启动项	★★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019年07月15日(总第191期)试行 本期4版 微信搜索：antiylab 内部资料 免费交流

广东省政协主席王荣率住粤全国政协委员考察安天总部

近日，广东省政协主席王荣带领住粤全国政协委员代表团在黑龙江省政协主席黄建盛的陪同下莅临安天总部参观指导。全国政协委员、安天创始人肖新光同来宾进行了汇报交流。

代表团参观了解了安天整体研发能力、核心引擎能力、高级威胁捕获分析能力、产品体系和解决方案等。重点听取了安天在安全解决方案中，通过“安全运维一体化”思路，全面改善信息资产的可管理性；研发战术性态势感知平台，指挥控制积极防御体系等方面的工作实践汇报。了解了安天产品和解决方案在重要信息系统和关键信息基础设施的部署情况和效果。来宾对安天的技术实力和安全理念给予了充分的肯定。

根据党中央、国务院关于实施新一轮东北地区等老工业基地振兴战略的决策部署，黑龙江省和广东省建立了对口合作机制，哈尔滨和深圳结成了对口城市。两地交流频繁，合作样板项目逐渐成型。

肖新光表示，安天很早就建立了深圳研发中心，在粤港合作的大背景下，安天与广州大学建立了网络空间高级威胁对抗联合实验室，积极投入深圳鹏城实验室网络靶场等项目建设；感谢广东相关单位对安天的支持，期待与更多广东企事业单位合作，也期待广东企业向东北振兴投入更多资源，合作共赢。

安全厂商披露恶意软件 Powload 逃避技术

Powload 恶意软件通常被用作其他恶意软件的辅助载荷，因其能够将简单的感染方法与不断发展的规避手段结合而被广泛使用，其中最典型的就是银行木马 Emotet。趋势科技研究人员通过分析 5 万多个样本，了解到 Powload 如何使用新技术来提高其效率以及逃避检测的方法。典型的 Powload 攻击使用社交工程让用户点击电子邮件附件（通常包含 VBA 编码的宏），隐藏的 PowerShell 进程以下载和执行恶意软件载荷。Powload 使用的逃避手段主要包括：使用基于 XML 的文档来逃避检测；利用 Forms 模块隐藏恶意宏字符串；使用受密码保护的宏模块；可能使用隐藏的 VBA 项目模块。（原文链接：https://blog.trendmicro.com/trendlabs-security-intelligence/powload-loads-up-on-evasion-techniques/）

利用 Windows 提权漏洞的零日攻击针对东欧

2019 年 6 月，ESET 研究人员发现利用 Windows 中的本地权限提升漏洞的零日攻击高度针对东欧国家。此漏洞创建了两个窗口，分别在第一和第二阶段使用，第一个窗口创建弹出菜单对象并使用 CreatePopupMenu 和 AppendMenu 函数追加菜单项。漏洞利用程序还设置了 WH_CALLWNDPROC 和 EVENT_SYSTEM_MENUPOPUPSTART 挂钩，漏洞利用程序调用 TrackPopupMenu 函数显示一个菜单，然后执行连接到 EVENT_SYSTEM_MENUPOPUPSTART 的代码，通过向菜单发送消息序列打开第一个可用项。至关重要的一步是初始菜单已创建但子菜单尚未创建的时候处理 WH_CALLWNDPROC 钩子中的 WM_NCCREATE 消息，然后发送消息取消该菜单。攻击者使用第二个窗口是翻转第二个窗口的 tagWND 结构中的 bServerSideWindowProc 位。这导致在内核模式下执行 WndProc 过程。（原文链接：https://www.welivesecurity.com/2019/07/10/windows-zero-day-cve-2019-1132-exploit/）

微软发布七月安全更新修补两个零日漏洞

微软发布七月安全更新，包括 1 个建议、1 个服务堆栈更新和 77 个漏洞的更新，包括两个零日漏洞。CVE-2019-1132 是 Win32k 特权提升漏洞，攻击者可利用该漏洞以内核模式运行任意代码，可以安装程序，查看、更改或删除数据，以及创建具有完全用户权限的新帐户。CVE-2019-0880 是 Microsoft splwow64 特权提升漏洞，由 ReSecurity 的 Gene Yoo 发现。（原文链接：https://www.bleepingcomputer.com/news/microsoft/microsofts-july-2019-patch-tuesday-fixes-2-zero-day-vulnerabilities/）

Pale Moon Windows 档案服务器感染恶意软件

Pale Moon 网络浏览器团队称其 Windows 档案服务器遭到破坏，黑客在 2017 年 12 月 27 日用 Win32 / ClipBanker.DY 木马感染了 Pale Moon 27.6.2 及之前版本的所有安装程序，下载 Pale Moon 浏览器安装程序和自解压存档的用户将感染恶意软件。根据 Pale Moon 数据泄漏验证，Pale Moon 的主要分销渠道不受影响，只有顶级服务器上的 .exe 文件受到影响，存档内的文件不会被修改。（原文链接：https://www.bleepingcomputer.com/news/microsoft/microsofts-july-2019-patch-tuesday-fixes-2-zero-day-vulnerabilities/）

每周安全事件

类 型	内 容
中文标题	新 Trickbot 木马部署自定义代理模块 IcedID
英文标题	Trickbot gets custom proxy module from IcedID banking trojan
作者及单位	Malware and Vulnerabilities
内容概述	研究人员发现 Trickbot 木马部署了自定义代理模块 IcedID，代理模块可以拦截和修改 Web 流量，充当客户端和在线银行服务之间的本地代理服务器，并且包括窃取财务信息的虚假用户请求模板。研究人员表示此代理模块可以连接到谷歌浏览器，包括 Mozilla Firefox、Internet Explorer 和 Microsoft Edge。
链接地址	https://cyware.com/news/trickbot-gets-custom-proxy-module-from-icedid-banking-trojan-470f9c2e

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.ScaryGranny.a[prv,pay,fra] 2019-07-07	高	该应用程序包含恶意代码，运行后加载钓鱼界面，诱导用户填写 google、Facebook 账号和密码，并将用户登录凭证上传，以免费的名义诱导用户点击付费购买。造成用户隐私泄露和经济损失，建议立即卸载。
		RiskWare/Android.facaizhu.a[exp] 2019-07-08	中	该应用程序为互联网金融服务平台，目前该公司已因非法吸储被警方通报，可能没有财产权益保障，造成用户财产损失，建议不要使用。
		RiskWare/Android.huirongtech.a[prv,exp] 2019-07-09	中	该应用程序是测试应用，包含获取短信和安装列表以及发送短信的风险代码，可能会造成用户资费损耗，请谨慎使用。
	较为活跃样本	Trojan/Android.CoreSpy.a[prv,spy]	中	该应用程序是一款间谍软件，运行后隐藏图标，后台窃取用户短信、联系人、通话记录、浏览器记录、地理位置、手机应用安装信息、sim 卡相关信息，私自进行通话录音、拍照、摄像，并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。
		Tool/Android.waladifin.a[prv,rmt]	中	该应用程序是一款监控应用，包括检测报警、定位跟踪、视频监控、远程录像、强制响铃等功能，建议谨慎使用，非自主安装建议卸载。
		Trojan/Android.cwtcn.a[prv,rmt,bkd]	中	该应用程序伪装系统安全服务，安装无图标，后台接收控制指令，监听用户通话，静默拍照、录音、录像，窃取用户地理位置，统计用户应用使用时间、通话时间。并将数据上传至服务器。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.ContactSpy.b[prv]	低	该应用程序运行会获取用户手机号码与通讯录，联网执行上传操作，会造成用户隐私泄露，请及时卸载该程序。
		Trojan/Android.ankubist.a[prv]	低	该应用程序运行获取用户通讯录，通话记录以及短信并上传，造成用户隐私泄露，建议卸载
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows 安全特征绕过漏洞（CVE-2019-1019）	高	Windows 中 Netlogon 消息能够获取会话密钥并对消息进行签名，该消息存在一个安全特征绕过漏洞。为了利用此漏洞，攻击者可以发送精心设计的身份验证请求。成功利用此漏洞的攻击者可以使用原始用户权限访问另一台计算机。
	较为活跃样本	Trojan[Backdoor]/PHP.IRCBot	中	此威胁是一种使用 PHP 脚本语言编写并存在后门的木马类程序。它可以连接到 IRC 服务器，并允许黑客远程控制用户电脑。该家族最终会将用户电脑变成一个广告现金制造机。该家族需要手动安装，它通过即时通讯软件、Facebook、恶意网站等方式进行传播。通常该家族会伪装成图片，看上去很真实，但是当你仔细观察，你会发现它是一个可执行程序。
		Trojan[Ransom]/NSIS.Onion	中	此威胁是一种使用 Nullsoft 安装框架进行打包的木马家族。该家族的样本在执行后会安装捆绑在其中的勒索软件，加密用户的文档并留下勒索信向用户勒索解密文件的赎金。
		Trojan[Downloader]/JS.Psyme	中	此威胁是一种以 Javascript 文件为载体的木马家族。该家族的样本具有下载行为。该家族的样本在执行后会下载其它恶意程序并执行。
		GrayWare[AdWare]/Win32.Look2Me	低	此威胁是一种广告件行为的灰色软件家族。该家族的样本在执行后会监视系统行为、在网络上下载广告部件、在用户的通知中心弹出内容并使用特定的 DLL 文件来隐藏自身。
		RiskWare[RiskTool]/OSX.ExtInstall	低	此威胁是一种风险软件类程序。该家族样本为恶意扩展安装程序，有一定的威胁性。

为何说“身份管理”是安全的基础

Rob MacDonald/ 文 安天技术公益翻译组 / 译

曾几何时，公司保护高价值信息的方法是：将重要文件锁在保险柜中，为公司的数据库和计算机系统设置口令和防火墙，或许还安装摄像头来监控办公区域。

那样的日子已经一去不复返了。如今，边界日渐消亡，保护边界已经成为了一项不可能完成的任务。

虽然企业的一些信息仍然托管在内部服务器上，但是大部分信息已经迁移到云端。Flexera 公司最近的一项研究显示，84%的企业已经采用了多云策略，而且公有云的采用率超过私有云。

即使企业的数据是本地存储的，其员工也可以在家中访问这些数据，或者在会议上和机场等场所用智能手机访问数据。如今，公司不仅雇用常规的坐班员工，还雇用其他地区和国家的承包商——如远在印度或菲律宾的承包商。这些承包商（服务技术人员）负责管理企业的 IT 系统，而这些系统中存储着企业竞争对手试图获得的数据。

在这么多人能够访问企业应用、数据库和系统的情况下，保护企业数据的唯一可靠方法是对访问者进行“身份管理”。

该方法不仅适用于企业本地的系统和应用，也适用于软件供应商管理的云服务。由于缺乏对云应用安全性的可见性，企业无法管理其风险——但是一旦企业数据遭泄露，企业就要承担责任。为了避免这种情况，企业应对访问者进行身份管理。

什么是身份管理？

身份管理是指：确保任何试图访问企业信息的人都获得了授权。如果被访问的信息非常重要，企业可以全程监控访问者，以确保他们只执行被授权的操作。

企业应根据访问者的角色确定其访问权限。在员工或承包商登录企业系统之前，企业应预先确定他们可以访问哪些应用和数据库，以及他们可以对这些应用和数据库执行哪些操作，如仅读取信息、更改或下载信息等等。

当有人登录时，在对其授权之前，需要鉴别他是否是所声称的那个人。如果此人试图访问敏感信息，那么在当今复杂的安全环境中，仅仅鉴别其用户名和口令是不够的。企业需要进行多因子身份鉴别，如令牌、短信验证码、软件和生物识别扫描。如果用户通过了多因子身份鉴别，且其访问权限受到企业身份和访问管理系统的限制，那么他应该是合法用户。

但是，如果该用户暂时从电脑旁走开，而其他人使用了他的电脑呢？为了防止这种情况，每当用户离开设备，导致设备无人看管时，企业都需要锁定设备的屏幕。

就这样吗？当然不是。企业还应实时监控涉及高风险站点和数据库的所有会话。

这种监控经常与应用和数据库的监控相混淆。当然，应用和数据库系统应配备防火墙来阻止入侵者。如果有人试图冲破防火墙，安全中心就会收到告警通知。

但是，如果被授予访问权限的人决定做坏事，那防火墙就无济于事了。会话监控是指全程监控访问数据的人；如果此人试图执行可疑的操作——如泄露客户信息，企业的安全中心将会立即收到通知，并在其窃取信息之前切断其访问权限。

“物”也有身份

到目前为止，我们一直在讨论如何管理“人”的身份和访问权限。但是，“物”也是有身份的。

企业的 IT 部门可能设置了服务账户，以便在系统内或系统之间执行任务。就像人一样，这些账户可以访问敏感信息。这些账户在使用过程中应进行管理和监控，在使用之后也应进行监控。

监控服务账户可能听起来很荒谬。毕竟，“账户”不是“人”，无法自行窃取信息并在互联网上售卖这些信息。

但是，入侵这些账户的黑客可以窃取和售卖信息。事实上，黑客很喜欢这些账户——这是因为企业将此类账户视为执行任务的“机器”，通常不会关注它们。

随着物联网（IoT）的发展，对服务账户和机器人的管理和监控越来越重要。从工厂机器人到智能汽车和恒温器，再到能够订购食品的冰箱，嵌入传感器的机器配备了越来越多的功能。Gartner 称，到 2020 年，IoT 市场将涵盖 208 亿台联网设备。

对于 IT 部门来说，这些“物”需要与“人”一样对待。如果它们包含黑客想要的敏感信息，则需要以适用于人类账户的警惕级别对它们进行管理和监控。

随着世界的迅速变化，安全技术也必须进行改变。最好的系统不仅能为企业提供最先进的保护，而且还具有适应未来的灵活性。

原文名称	Why identity is the foundation of security
作者简介	Rob MacDonald。Rob MacDonald 是 Micro Focus 公司解决方案战略总监。
原文信息	2019 年 7 月 8 日发布于 Help Net Security。 原文地址 https://www.helpnetsecurity.com/2019/07/08/why-identity-is-the-foundation-of-security/
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。