安天智甲有效防护 Cinobi 窃密木马

近日，安天 CERT 在梳理网络安全事件时发现一个活跃的 Cinobi 窃密木马。Cinobi 窃密木马主要通过垃圾邮件、漏洞利用、钓鱼网站进行传播。该窃密木马主要功能是窃取银行账户登录凭证。

攻击者使用钓鱼网站诱使受害者点击名为“index.clientdownload.windows” 的按钮，之后登录页面开始下载 zip 压缩文件，压缩包包含 LogiCapture.exe、cfg.config、config.dll、format.cfg 和 Xjs.dll 等文件。攻击者利用了白加黑技术反查杀。当受害者运行正常文件 LogiCapture.exe 时，加载 Xjs.dll 文件，Xjs.dll 从 format.cfg 中获取并运行 ShellCode，ShellCode 加载 config.dll 从 cfg.config 获取并运行新 ShellCode，新 ShellCode 下载 Tor 程序压缩包并安装 Tor 浏览器，之后下载并加载随机命名的 dll 文件，dll 连接 C&C 服务器下载并安装窃密载荷，窃密载荷通过获取浏览器存储的相关信息，从而窃取银行账户登录凭证。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不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良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，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窃密木马的鉴定；安天智甲已经实现了对该窃密木马的查杀。

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，下为其自动生成的分析报告：

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(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（WinXP）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、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	Xjs.dll
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	33 KB
MD5	7D602363A760AC03092DF5A2FFD774D6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=7D602363A760AC03092DF5A2FFD774D6

◆元数据信息

描述	值
File Size	33 kB
File Type	Win32 DLL
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2021:06:24 14:26:59+08:00
PE Type	PE32
Linker Version	10.0
Code Size	18432
Initialized Data Size	14336
Uninitialized Data Size	0
Entry Point	0x13a9
OS Version	5.1
Image Version	0.0
Subsystem Version	5.1
Subsystem	Windows GUI

◆运行环境

操作系统	内置软件
Win7sp1 x86 旗舰版 service Pack 1	默认、IE8、Google Chrome、Firefox、Office2013、Flash、FoxitReader、Adobe Reader DC

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
疑似桌面控制	★

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2021年09月13日(总第295期)试行 本期4版 扫描上方二维码查询安天所有对外开放资料

安天连续七届蝉联国家级应急服务支撑单位 并入选首批 APT 监测分析名单

近日，国家互联网应急中心（CNCERT）经过公示发布了第九届 CNCERT 网络安全应急服务支撑单位入选名单，13 家国家级、78 家省级、8 家 APT 监测分析、5 家反网络诈骗企业入选该名单。安天连续七届十四年入选“国家级”应急服务支撑单位，同时入选首批 APT 监测分析单位。安天始终坚持支撑战略客户达成威胁对抗、安全防护与数字化融合闭环的愿景和努力，再次受到主管部门的检验和肯定。

加强能力建设，担当起国家级网络安全应急服务支撑责任

网络安全应急服务支撑单位是我国网络安全应急体系的重要组成部分。安天作为中国网络安全应急响应体系中重要的企业节点，忠诚履行作为 “网络安全国家队”的使命责任，打造了“第一时间启动，同时应对多线威胁，三体系联动，四作业面协同”的应急体系。为增强对重大、突发网络安全事件的应对能力，安天建立了一支综合高效的应急支撑服务队伍，通过自主创新、前沿技术研究、威胁情报获取、安全服务等一系列能力建设，随时应对及解决突发的网络安全事件。

持续分析曝光高级威胁，入选 APT 监测分析名单

安天长期坚持为 CNCERT 及各分中心提供高级持续性威胁（APT）深度分析、恶意代码监测信息共享与分析、安全漏洞信息报送与处置、网络安全信息报送、网络安全应急处置支撑及网络安全专项工作等多个维度的应急服务支撑。安天持续跟踪分析重大漏洞、恶意代码和 APT 组织的行动线索。对重大 APT 事件成功实现了前期储备，适时曝光，对恶意代码、网络威胁及时发现、及时上报主管部门，及时处置和响应。成功入选首批 APT 监测分析名单。

坚持“民企国家队”使命，构筑有效安全产品建设

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。在漏洞检测、威胁响应领域，安天拥有专业的研发团队和过硬的漏洞分析能力，除了积极配合主管部门和向公众的漏洞上报、披露的工作，安天近年来不断建立健全漏洞发现、上报、分析和处置工作机制，还从产品、服务等方面提升漏洞安全风险防范及应对能力，推动构建漏洞发现和处置生态环境。

近年来，安天巩固了威胁检测引擎、高级威胁分析对抗、海量威胁自动化分析和威胁情报等方面的基础能力优势。构筑了由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品品牌方阵，可以为客户构建资产运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置、可信接入等基础安全能力。

2021 年初，安天对外发布了新版的价值主张：依托端到端的安全能力和供应链关口前移的优势，实现全场景的有效防御覆盖与可信场景构造。并依托强大的威胁对抗体系，实现深度客户赋能，驱动客户完成从威胁情报消费，到自主安全能力生产的智能化安全运营变革。

我们支撑战略客户达成威胁对抗、安全防护与数字化融合闭环的愿景，我们的能力是国家网空战略防御能力的基石，是社会安全治理的保障，是维护网络空间人类命运共同体安全的支撑力量。

未来，安天将继续全力配合 CNCERT 和各分中心做好网络安全应急服务支撑工作，积极开展恶意代码监测分析与追踪溯源、威胁情报分析、威胁深度分析、APT 事件跟踪、应急响应服务等多个方面紧密合作，助力国家公共互联网网络安全应急体系建设。（原文链接：https://mp.weixin.qq.com/s/itknDoYqV2Q6VaNgplgS4g）

扫描右侧二维码阅读全文

让网赚“正经”起来，从规范通知栏乱象开始

网赚，作为一种新兴的赚钱方式已经被越来越多的人接受，也被越来越多的人认可。也正因此，网赚 App 打着“做任务赚佣金，边玩手机边赚钱”等口号吸引了不少用户注册使用。

据“App 治理工作组”2020 年 7 月披露的信息：App 专项治理工作组“App 个人信息举报”举报平台收到的有效举报信息中，近期内涉及“网赚”类 App 的举报信息就高达 200 余条，大部分都涉及利用套路骗取个人信息等问题。

现象：网赚 App 中广泛存在通知栏消息推送乱象

随着智能手机的普及，手机 App 的消息通知推送功能中无效信息量大增，已经如垃圾短信一般骚扰用户的日常使用，影响用户体验。通知栏这个本是为了提高用户获取信息效率的位置，现在却成了 App 推送的“垃圾场”。

在持续关注和披露当前移动应用侵害用户权益行为的过程中，安天移动安全风险检测预警平台发现，网赚 App 作为用户量非常可观的品类，除了侵害用户权益进行广告变现，存在威胁个人信息安全相关行为外，还广泛存在滥用通知栏推送的现象。（原文链接：https://mp.weixin.qq.com/s/GdE36gNXVKFnfaZfRV80rA）

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	FIN7 黑客利用 Windows 11 主题文档传播后门
英文标题	FIN7 Hackers Using Windows 11 Themed Documents to Drop Javascript Backdoor
作者	Ravie Lakshmanan
内容概述	最近的一波鱼叉式网络钓鱼活动利用带有 Visual Basic 宏的武器化 Windows 11 Alpha 主题 Word 文档，针对位于美国的销售点 (PoS) 服务提供商投放恶意载荷，包括 JavaScript 植入程序。据网络安全公司 Anomali 的研究人员称，这些攻击被认为发生在 2021 年 6 月下旬至 7 月下旬，归因于一个名为 FIN7 的威胁行为组织。感染始于 Microsoft Word 恶意文档，其中包含一个据称是“在 Windows 11 Alpha 上制作的”诱饵图像，敦促接收者启用宏以触发下一阶段的活动，其中包括执行一个严重混淆的 VBA 宏，用于检索 JavaScript 载荷。VB 脚本还会检查它是否在虚拟环境下运行，如 VirtualBox 和 VMWare，如果是，就停止感染链。在检测到俄语、乌克兰语或其他几种东欧语言时，也会停止感染。
链接地址	https://thehackernews.com/2021/09/fin7-hackers-using-windows-11-themed.html

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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称	威胁等级	简要描述
活跃漏洞	Microsoft MSHTML 远程代码执行漏洞（CVE-2021-40444）	高	Microsoft MSHTML 存在远程代码执行漏洞。由于 MSHTML 组件中的输入验证不当，使得远程攻击者可以创建带有恶意 ActiveX 控件的特制 Office 文档，诱使受害者打开文档并在系统上执行任意代码。
	Advantech WebAccess 缓冲区错误漏洞（CVE-2021-38408）	高	Advantech WebAccess 存在缓冲区错误漏洞，该漏洞源于缺乏对用户提供的数据长度的正确验证而导致的基于堆栈的缓冲区溢出。该漏洞可能允许远程代码执行。
	WordPress 安全漏洞（CVE-2021-38312）	高	WordPress Gutenberg Template Library & Redux Framework plugin 4.2.11 版本存在安全漏洞，该漏洞源于在 REST 路由下注册的 REST API 端点中使用了错误的授权检查，攻击者可以从 WordPress 存储库安装任意插件并编辑任意帖子。
较为活跃样本家族	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	Trojan[Backdoor]/Win32.Finfish	中	该病毒家族是一种可以窃取用户信息的木马类程序。该家族样本运行后修改注册表使其自启动，窃取用户敏感信息，如帐号密码等。
	Trojan[DDoS]/Linux.Xarcen	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要利用漏洞和弱口令对 IoT 设备进行攻击并组建僵尸网络，利用该僵尸网络对任意目标发动 DDoS 攻击。
	Trojan/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

增强企业安全态势的三种方法

比尔·富兰克林 / 文 安天技术公益翻译组 / 译

随着新冠病毒变种的增多，员工远程办公的时间可能会远超 IT 领导者的预期，这会增加网络攻击的风险。这些攻击可能会导致客户数据泄露、公司信息遭窃或内部运营被控制等等。更糟糕的是，攻击的增加正值企业网络安全专家短缺之际——截至 2020 年，网空安全专家的缺口高达 300 万。

在这种情况下，企业面临着巨大的困境——安全比以往任何时候都更加重要，但是其网络安全专家几乎无法获得补充。幸运的是，企业可以遵循一些安全最佳实践来增强其安全态势。

增强安全态势的三种方法

下述三个最佳实践可以帮助企业增强安全性。

1. 建立授权保障

即使是最小的安全漏洞也有可能会被网络犯罪分子利用，以访问企业网络。我们以燃油管道公司 Colonial Pipeline 攻击事件为例，攻击者利用泄露的口令入侵了一个非活动授权账户，由此入侵了公司网络并访问公司数据。由此可见，IT 领导者必须创建适当的授权协议，以防止 Colonial Pipeline 类攻击发生在他们身上。

企业必须立刻（而非几小时、几天或几周后）处理明显的安全漏洞，例如新的非活动授权账户或对授权账户的网络钓鱼攻击等。事实上，根据 Verizon 公司的一份报告，在涉及黑客攻击或暴力破解的数据泄露事件中，有 80% 是利用丢失或被盗的员工凭证侵入公司系统的。而 75% 的“常见”数据安全漏洞是由特权滥用（员工可以不受限制地访问系统，即使不是为工作所需）导致的。

企业需要创建授权协议，例如多因子身份验证、定期更改口令和最低权限用户访问等，以减少网络犯罪分子不受限制地访问其系统的可能性。

企业领导者可能担心，要求员工遵循授权最佳实践来访问敏感信息会花费太多时间，这会减慢内部运营。但是需要注意，一旦遭到攻击，企业的运营就会被严重扰乱，这可比多花点时间严重多了。

2. 进行加密

加密是指使用算法使数据或其他信息成为不可读的密码，如果没有正确的加密密钥，就无法解密这些密码。因此，加密可以确保，只有正确的接收者才能访问信息。

加密密钥管理——创建、存储、删除和销毁加密密钥的过程——有助于企业实现对敏感信息的安全访问。通过建立密钥访问，信息不会直接保存在系统中，密钥可以由企业随意更改。

在没有加密密钥的情况下，攻击者很难猜测发件人用于加密消息的密码，以及使用哪些密钥作为变量。因此，加密是防御网络攻击的重要工具。

可以自动预激活、激活、更改和重新分配加密密钥的解决方案，可以帮助各种规模的企业使用加密技术。即使没有网络安全专家，企业也可以采用此类解决方案。但是，企业应依靠具有资源、网络和经验的、供应商中立的可信赖顾问，以确保其加密密钥管理解决方案能够满足需求。

3. 使用 DRaaS（灾难恢复即服务）解决方案

网络安全的真正含义可以归结为“准备就绪”，尤其是在发生攻击的情况下。如果企业遭受网络攻击且敏感信息遭窃取，则灾难恢复计划或解决方案有助于减轻损害。这就是“灾难恢复即服务” (DRaaS) 解决方案的用武之地，它会将服务器信息和数字业务运营复制到恢复站点上，以便在发生紧急情况、故障或系统损坏时进行备份，以替换主服务器。

此外，DRaaS 解决方案可以通过不可变备份进行强化，从而为企业基础架构增加另一层安全性。不可变备份能够保护数据，使其无法更改，为企业的灾难恢复解决方案建立一个固定的、不可删除的数据源。通过不可变备份，企业就拥有了用于恢复的固定源，攻击者就难以永久删除或更改数据。

通过 DRaaS 解决方案，网络犯罪分子造成永久性损害或拥有敏感数据唯一所有权的可能性会被大大降低。如果没有此类解决方案，网络犯罪分子就有可能劫持企业数据并干扰业务运营、泄露敏感信息，甚至在企业无法满足其要求时销毁数据。

尽管企业目前缺乏网络安全人才，且网络攻击处于历史最高水平，但他们仍然可以增强其安全态势。通过将主动安全措施与灾难恢复解决方案相结合，企业可以降低攻击成功的可能性。

原文名称	3 ways to protect yourself from cyberattacks in the midst of an IT security skill shortage
作者简介	比尔 · 富兰克林（Bill Franklin），是 AVANT 公司的云工程高级总监。
原文信息	2021 年 9 月 6 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/09/06/protect-yourself-from-cyberattacks/
摘 要	企业面临着巨大的困境——安全比以往任何时候都更加重要，但是其网络安全专家几乎无法获得补充。幸运的是，企业可以遵循一些安全最佳实践来增强其安全态势。这些实践包括：（1）建立授权保障；（2）进行加密；（3）使用 DRaaS（灾难恢复即服务）解决方案。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。