AZORult 窃密木马分析报告

近日，安天 CERT 在梳理网络安全事件时发现一个名为 AZORult 的窃密木马。该窃密木马最早在 2016 年 7 月被发现，至今多次更新，主要通过钓鱼邮件和 RIG 漏洞利用工具包进行传播，目的是窃取用户凭据和帐户。

本次分析样本是通过钓鱼邮件进行传播，邮件附件为带有密码的压缩包，诱导用户手动输入解压密码查看附件，附件解压后释放出一个含有 CVE-2017-11882 Microsoft Office 公式编辑器漏洞的 Office 文档，一旦用户执行便会连接 C2(hxxp://vektorex.com/source/Z/15603887.png) 下载最终载荷 AZORult 窃密木马。该木马运行后将自身添加到注册表实现开机自启动，AZORult 窃密木马的主要功能为窃取银行密码、信用卡、浏览器历史记录以及数字货币等信息，将窃取的信息上传至 C2(hxxp://bixtoj.gq/sc01/index.php)。

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、安全云鉴定器、字符串分析鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（Win7sp1 x86）鉴定器、动态（WinXP）鉴定器、文件相似分析鉴定器、信标检测鉴定器、智能学习鉴定器、静态特征检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	75be.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.07 MB
MD5	35D3FFD9CE2E315C23A0842B40568047
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ekstak
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=35D3FFD9CE2E315C23A0842B40568047

◆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、Office2003、Flash、WPS、FoxitReader、AdobeReader

◆信标信息

信标类型	信标内容	检测结果
domain	bixtoj.gq	未知
mutex	AB419DE5-3231ABE6-BF235135-47DAA2AC-61E97632A	未知

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★
向其他进程内存写入数据	★★★
自启动	★★★
创建互斥量	★★★
发送 http 数据	★★★★

◆常见行为

行为描述	危险等级
使用 windows COM 库 API	★★
创建挂起进程	★★
读取自身	★★
创建可执行文件	★★
镜像劫持	★★
收集操作系统硬件信息	★★
加载运行时 DLL	★
获取系统版本	★
加载资源模块	★
创建窗口	★
.....	.....

◆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 06 月 21 日 (总第 283 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

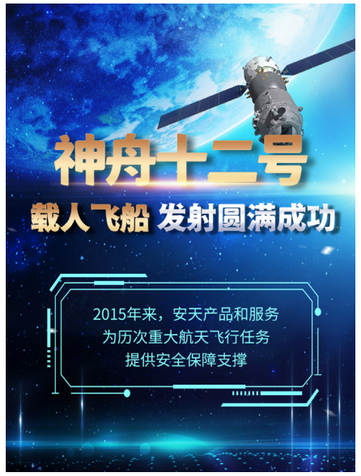
安天网络安全产品保障神舟十二号载人飞船发射

北京时间 2021 年 6 月 17 日 9 时 22 分，搭载神舟十二号载人飞船的长征二号 F 遥十二运载火箭，在酒泉卫星发射中心点火发射。15 时 54 分，神舟十二号载人飞船与天和核心舱完成自主快速交会对接。18 时 48 分，航天员进入天和核心舱，标志着中国人首次进入自己的空间站。这是我国载人航天工程立项实施以来的第 19 次飞行任务，也是空间站阶段的首次载人飞行任务。

此次发射任务中，安天相关网络安全产品提供了安全检测防护能力，保障系统安全运行。2015 年以来，安天产品和服务为历次重大航天飞行任务提供安全保障支撑，包括天舟一号飞行任务、长征五号 B 运载火箭首次飞行任务、“珠海一号”03 组卫星发射任务、“探月工程”等，安天的工程师们和安天系列安全产品为发射、飞控等场景安全提供了网络安全保障，多次收到相关部门感谢信。

（原文链接：https://mp.weixin.qq.com/s/xCp2dvfMzpd9Zy3htPNE2w）

扫描右侧二维码阅读全文



安天在哈举行 2021 集团干部培训班

2021 年 6 月 5 日至 7 日，安天集团干部培训班在哈尔滨举行。安天集团创始人、董事长肖新光，执行董事长、CEO 游小明与“光明组合”管理团队，来自集团六地研发中心、四大营销事业部、集团总部各职能部门的负责人和业务骨干，以及安天移动安全公司、国泰网信的核心高管，共 150 余人参加了培训。

▲ 安天集团创始人、董事长肖新光讲话

2021 年 6 月 6 日，是安天创业 21 周年，安天集团创始人、董事长肖新光在干训班开训仪式上作了《不负历史，达成未来》的讲话，从共创、共享、使命三个维度，系统总结了安天创业历史和技术创新基因、介绍了合伙人机制设计，强调全体干部要坚守创业初心、牢记网络安全国家队使命，达成客户有效安全价值。

▲ 安天执行董事长、CEO 游小明讲话

安天执行董事长、CEO 游小明在干训班总结时作了《求变图强取大势，凝聚人心创未来》的主题演讲，回顾了安天创业 21 年不忘初心、坚持坚守，树立起国内外网络安全业界高技术品牌的发展历程；在研判网络安全领域发展趋势基础上，提出了未来发展的“335 规划”和“四化战略”转型思路，并对 2021 年度目标和重点工作进行了部署。鼓励安天干部团队和业务骨干要梦想叠加、共创共享，主动求变、踏实高效，在传承安天优秀文化的基础上与时俱进、兼容并蓄，坚持高质量地服务客户，最大化地保障安全价值。

安天产线负责人对全体参训人员进行了新版政企场景产品和服务板块划分培训。安天打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足用户对于包括终端杀毒、EPP、EDR、CWPP 等系统安全层面需求。整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力。基于流量产品探海可以有效应对用户对于 NDR 和 NTA 的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到 APT 攻击的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

面对全新场景和客户的数字化转型，安天提出了“超越产品赛道，重构有效安全价值”的产品发展导向，围绕识别、塑造、检测、防护、响应关键能力动作与客户场景的结合，实现按需组装。（原文链接：https://mp.weixin.qq.com/s/eYW-CU6PtlgDmRkRQFMosA）

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	加拿大多伦多亨伯河医院遭到勒索软件攻击
英文标题	‘Humber River Hospital’ Shuts Down Essential Services Due to Ransomware Attack
作者	Bill Toulas
内容概述	加拿大多伦多的“亨伯河医院”（Humber River Hospital）遭受了勒索软件攻击，该医院发布声明解释说，攻击发生在 2021 年 6 月 14 日，也就是系统打过补丁并应用了所有最新更新的一天之后。这意味着用于攻击的恶意软件使用了一个零日漏洞，但没有提供这方面的更多细节。医院的 IT 团队关闭了所有的 IT 系统，包括患者的健康记录——虽然一些文件已经损坏，但绝大多数数据仍未受到影响。
链接地址	https://www.technadu.com/humber-river-hospital-shuts-down-essential-services-ransomware-attack/283978/

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 Office Graphics 远程代码执行漏洞（CVE-2021-31940）	高	Microsoft Office Graphics 存在远程代码执行漏洞。由于 Microsoft Office Graphics 中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件或访问恶意网站并在目标系统上执行任意代码。
	Microsoft 3D Viewer 存远程代码执行漏洞（CVE-2021-31942）	高	Microsoft 3D Viewer 存在远程代码执行漏洞。由于该应用中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件或访问恶意网站并在目标系统上执行任意代码。
	Windows MSHTML Platform 远程代码执行漏洞（CVE-2021-33742）	高	Windows MSHTML Platform 存在远程代码执行漏洞。由于在 Windows MSHTML Platform 中处理 HTML 内容时出现边界错误，使得攻击者可以创建一个特制的网页，诱使受害者打开它，触发内存损坏并在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Ransom]/Win32.Crypmodadv	高	此威胁是一种勒索软件家族。该家族的样本在运行后，会加密系统上多种文件格式的文 件，并将文件的扩展名更改为 .remind。在加密后，该样本会在全部的文件夹下各放置 一封 HTML 格式的勒索信说明情况。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	Trojan/Win32.Scar	中	此威胁是一种木马类程序，可以将某些金融网站重定向到攻击者设置的另一个地址，模仿登录界面从而窃取用户密码。
	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/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan[Dropper]/Android.Wroba	中	此威胁是安卓平台上的一种恶意代码释放类木马家族。该家族木马运行后激活设备管理器、隐藏图标。接收短信指令，根据指令拦截指定短信，伪造新版本通知释放恶意 apk 同时卸载正常程序，上传手机用户隐私信息至远程服务器地址。

了解云共享责任模型

阿米奇·蒂瓦特 / 文 安天技术公益翻译组 / 译

在过去的一年中，企业不得不快速过渡到远程工作，因此他们开始进行云迁移。但是，在许多情况下，他们优先考虑实用性而非安全性，以避免业务中断，这导致很多企业存在漏洞。

出现这些漏洞的一个重要原因是：很多企业依赖于云提供商的默认安全服务，这些服务通常作为“自己动手”工具包和指南提供，用户需要自己进行实际配置。

如今，在“云优先”环境中，企业在与云提供商的“共享责任模型”下运作，该模型列出了哪些职责属于云提供商以及哪些职责属于用户。虽然共享责任模型的概念比较容易理解，但是实施起来需要进行大量的协调。

在许多情况下，共享责任模型确定：云提供商负责“云”的安全性，而企业负责“在云中”的安全性。这两者的区别可能有点令人困惑。举例来说：家庭安全提供商可以安装保护系统，但是房主需要确定传感器所在的位置，并确保在离开房子之前启动安全系统。同样，云提供商可以保护云的基础架构以降低入侵风险，而企业需要在发生攻击的情况下保护数据。

考虑到大多数企业在多个云环境中运作，问题就更加复杂了。Accenture 公司指出，93％的企业正在运行多重云策略，每家企业平均使用 3.4 个公有云和 3.9 个私有云。公司不仅需要定期分析和评估自己的安全态势，还需要定期分析和评估云提供商的安全态势。

现在，企业比以往任何时候都依赖于云。因此，他们必须创造一个环境，来履行其在共享责任模型下的职责。他们可以采取下述措施来保护数据。

1. 确定敏感数据：在将数据迁移到云中之前，企业应使用高级数据查找方法，查找其数据库中的敏感数据。考虑到“敏感数据”的范围在不断扩展，企业必须遵守隐私法规，这一点非常重要。例如，除了个人识别信息（PII，如社保号和出生日期）之外，IP 地址和地理定位信息现在也被视为敏感信息。

2. 确定数据的使用情况：企业应确定收集数据的目的，以遵守 GDPR 和 CCPA 等隐私法规。此外，企业应确定如何处理数据，并确定是否需要与第三方共享数据。最重要的是，企业应确保数据不会落入未经授权的人员手中，否则就会面临巨额罚款。

3. 分配访问控制：企业应确定“谁”能访问数据并对其进行处理。企业可以使用动态屏蔽工具，根据各自角色为员工创建自定义视图。例如，访问云中数据集的数据科学家和应用程序开发人员需要不同的视图。

4. 分析云提供商的安全资质：与其他服务提供商一样，云服务提供商也应提供可量化的证据，以证明其能够保障云安全。企业应对云服务提供商进行尽职调查，包括云安全资质，以及是否定期发布合规和审计报告等。

5. 寻求高级保护：通过将数据库迁移到云中，企业会在规模和可用性方面获得诸多优势，但是需要放弃对数据所在位置的控制。企业应始终了解“云服务提供商是否可以查看我的数据”，“是否会有人冒充云服务提供商的管理员查看我的数据”等问题。在这种情况下，“自带密钥”（BYOK）应运而生，成为一项日益受欢迎的技术解决方案，该技术可以帮助企业保持对数据（保存在他们不拥有的基础设施上）的控制权。

BYOK 对敏感数据记录进行加密或令牌化，以确保只有数据所有者可以访问它们。这些方法可防止云服务提供商访问数据。如果伪装为云服务提供商管理员的人员窃取了这些数据，那么他们只能得到加密的数据，并没有什么用。

传统的“静止”加密方法需要将数据存放在云中，在企业采取保护措施之前这些数据是裸奔的。采用内置于数据移动任务中的保护技术，可以消除该漏洞。

云计算已经是安全行业普遍接受的事实。因此，在进行云迁移之前，企业应了解云提供商的共享责任模型，并在数据的整个生命周期中（传输中，保存中和使用中）采取必要的保护措施。通过这些方法，企业可以降低攻击和不合规风险，同时获得云的诸多优势。

原文名称	Understanding the cloud shared responsibility model
作者简介	阿米奇·蒂瓦特（Ameesh Divatia），是 Baffle 公司的首席执行官。
原文信息	2021 年 6 月 15 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/06/16/cloud-shared-responsibility-model/
摘 要	云计算已经是安全行业普遍接受的事实。因此，在进行云迁移之前，企业应了解云提供商的共享责任模型，并在数据的整个生命周期中（传输中，保存中和使用中）采取必要的保护措施。通过这些方法，企业可以降低攻击和不合规风险，同时获得云的诸多优势。
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。