安天发布《Shade 勒索病毒分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Shade 的勒索病毒。Shade 勒索病毒首次出现于 2014 年末，主要针对美国，日本、印度，泰国和加拿大等地进行攻击，该勒索病毒对 Windows 操作系统有很强的破坏力，主要利用 Axpergle 和 Nuclear 漏洞工具包、钓鱼邮件等形式进行攻击。

在最近的一次攻击事件中，攻击者向受害者发送带有附件的钓鱼邮件，解压附件中的 zip 文件，实际上得到的是一个恶意的 JS 脚本，该脚本被攻击者进行了代码混淆，分析后发现该脚本会联网下载 Shade 勒索病毒样本。样本运行后首先将自身复制到系统目录下，伪装成系统文件并将自身设置为自启动。接着扫描系统文件，并加密上百种常见类型的文件，加密后的文件扩展名为 .crypted000007，如果所有文件都加密完成，勒索病毒会设置桌面背景为勒索提示信息，并且采用英俄双语提醒受害者电脑中的文件已经被加密，同时还会在桌面上创建 10 个内容完全相同的勒索信，勒索信内容也是采用英俄双语，并且攻击者提供了邮箱和 Tor 两种方式让受害者与其联系并支付费用获取解密密钥。

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、YARA 自定义鉴定器、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、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、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	f140cab283c35e92dc74db53b6d9964706538554d4151a637a406b093746692b
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.02 MB
MD5	CA84FED65ADF022BD0D2477EBCC2329F
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Shade
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=CA84FED65ADF022BD0D2477EBCC2329F

◆ 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
延时	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
壳行为填充导入表	★★
获取计算机名	★
获取系统信息（处理器版本、处理器类型等）	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
获取驱动器类型	★
隐藏文件	★
打开自身进程文件	★
读取自身	★★
释放 PE 文件	★
获取主机内存信息	★★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 06 月 03 日 (总第 185 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布关于海莲花组织针对移动设备攻击的分析报告

"海莲花"（又名 APT-TOCS、APT32、OceanLotus），被认为是来自中南半岛某国的 APT 攻击组织，自 2012 年活跃以来，一直针对中国的敏感目标进行攻击活动，是近几年来针对中国大陆进行攻击活动的最活跃的 APT 攻击组织之一。

安天及其他安全厂商在之前已经发布过多份关于海莲花的分析报告，报告的内容主要集中在 PC 端，攻击手段往往以鱼叉攻击和钓鱼攻击为主，移动端的攻击并不多见。然而，随着移动互联网的发展，一方面人们的手机逐渐出现两用性，除了包含使用者的个人隐私外，也往往会带有其社会属性，另一方面，智能手机的无线通信可以绕过内部安全监管设备，故而针对移动端的攻击也成为了整个攻击链条中的重要一环。下面，安天移动安全以发生于我国的一起移动端攻击事件为蓝本进行具体分析说明。

该应用伪装正常应用，在运行后隐藏图标，后台释放恶意子包并接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录等隐私信息，私自下载 apk、拍照、录音，并将用户隐私上传至服务器，造成用户隐私泄露。

安天移动安全团队对此次事件进行了详细的样本分析及拓展分析。（分析详情请扫描报告下方二维码查看。）

海莲花组织总是在演进变化，不断地通过更新其攻击手法和武器库以达到绕过安全软件防御的目的。除了武器库的不断更新，该组织也相当熟悉中国的情况，包括政策、使用习惯等。这不仅迷惑了相关人员，增加了其攻击成功率，同时也可能给目标受害群体带来不可估量的损失。因此对于个人来讲，要切实提高网络安全意识，不要被网络钓鱼信息所蒙蔽；对于安全厂商来讲，更需要对其加深了解并持续进行针对性的对抗，提升安全防护能力，真正为用户侧的移动安全保驾护航。

详情报告可扫描二维码阅读

黑龙江省新产业投资集团高尚国一行莅临安天参观考察

近日，黑龙江省新产业投资集团党委副书记高尚国、黑龙江省科力高科技产业投资有限公司董事长薄金峰、投资总监陈在奇等一行莅临安天哈尔滨总部参观考察。在展厅内，安天负责人向考察组介绍了安天的发展历程、安天获得的各项资质荣誉和在技术创新与专利技术方面取得的相关成果。同时展示了安天态势感知与监控预警平台以及其在普通场景及应急场景下的响应过程及分析、研判过程，并对安天智甲终端防御系统、探海威胁检测系统、追影威胁分析系统等安天能力型产品进行了介绍。

在参观过程中，考察组对安天的技术能力及取得的成果给予肯定，并针对安天的发展状况、业务布局等方面进行询问，并与安天相关负责人进行了详细交流。

Eaton 和 BlueCats 公司智能家居 App 中存在漏洞

Rapid7 研究人员披露了电力管理公司 Eaton 公司和物联网创业公司 BlueCats 智能家居产品中发现的一些重大漏洞。受影响的设备包括 Eaton 的 HALO 家庭智能照明系统和 BlueCats 的蓝牙传感器 AA Beacon。Eaton HALO 家庭智能照明系统的漏洞源于 Android 的 Halo Home 移动应用程序，该应用程序旨在将信息存储在设备上，然后应用程序可以访问该设备，这些信息可能泄露用户名或与个人帐户相关的详细信息。应用程序中的另一个漏洞有关不安全的直接对象引用（IDOR），只需知道到网页的直接链接任何人都可以访问某些用户记录，如电子邮件地址、通用唯一标识符（UUID）、移动设备版本和 MAC 地址。BlueCats AA Beacon 漏洞存在于用于连接设备的移动应用 BC Reveal，对于 iOS 和 Android 应用程序，BC Reveal 以明文形式存储设备所有者的名称和密码，攻击者可能通过某些物理攻击或恶意软件追踪敏感数据，并获得对受害者帐户的访问权限。

（原文链接：https://www.forbes.com/sites/ajdellinger/2019/05/28/researchers-disclose-vulnerabilities-in-popular-smart-home-apps-from-eaton-and-bluecats/#c12b20412c6d）

每周安全事件

类 型	内 容
中文标题	新西兰财政部遭到黑客入侵泄露预算文件信息
英文标题	NZ Treasury says systems 'hacked' ahead of Budget
作者及单位	Asha Barbaschow
内容概述	新西兰财政部长表示该部门有足够的证据表明受到黑客有意的入侵，其预算信息可能泄漏。财政部表示非常重视所有信息的安全性，发现事件后立即采取措施，增加所有与预算有关的信息的安全性，对信息安全流程进行全面审查，并且已根据国家网络安全中心的建议将此事提交给警方。目前没有证据表明财政部持有的任何个人信息受到影响。该国福利预算中列出的项目将于周四公布。
链接地址	https://www.zdnet.com/article/nz-treasury-says-systems-hacked-ahead-of-budget/

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

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.appvas.a[exp,rog] 2019-05-27	该应用程序包含恶意代码，监听拦截短信，下载并加载恶意子包，私自回复指定短信。造成用户资费损耗，建议卸载。（威胁等级中）
		RiskWare/Android.FakeJD.b[exp] 2019-05-28	该应用程序伪装京东，非官方应用，无实际功能，请用户谨慎使用，避免账号密码泄露。（威胁等级中）
		G-Ware/Android.ASTads.a[exp,rog] 2019-05-29	该应用程序运行动态加载内置的其他正常应用，后台推送积分墙、banner 广告，会造成用户资费消耗，建议不要使用。（威胁等级中国）
	较为活跃的样本	Trojan/Android.nguyen.a[prv,rog]	该应用程序运行后隐藏图标，后台私自屏幕录像并上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级低）
		Trojan/Android.KIASMSStealer.a[prv]	该应用程序运行后监听用户短信，窃取用户短信，私自更新联系人、并将用户短信上传至服务器。造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级低）
		Trojan/Android.HideMCOM.a[exp,rog]	该应用程序包含风险代码，运行后隐藏图标，后台加载广告，私自向指定号码发送短信。造成用户流量和资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.claveagil.a[prv,fra]	该应用程序伪装银行应用，运行后打开钓鱼界面诱导用户填写账号密码并上传，监听用户短信并上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Tool/Android.niuapp.a[prv,rmt,spy]	该应用程序是一款间谍工具，通过远程指令执行录音、录像、截屏、拍照、微信录屏、定位、隐藏图标等功能，还会备份短信、通话记录、通讯录等隐私信息上传到服务器，建议仔细阅读程序相关信息后使用，避免被恶意利用造成隐私泄露。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows DHCP 服务器远程代码执行漏洞（CVE-2019-0725）	当攻击者向 Windows DHCP 服务器发送经特殊设计的 DHCP 数据包时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在服务器上执行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Rootkit]/Boot.Wistler	该病毒家族是一种可以修改 MBR 并在系统内核之前加载的木马家族。该家族通过安装免费在线程序或第三方软件入侵用户电脑。该家族会修改系统设置及默认浏览器主页设置，弹出广告窗，使浏览器重定向至其他网页。该家族会为黑客打开后门，允许黑客窃取用户的信息。（威胁等级中）
		Trojan[Exploit]/HTML.DialogArg	该病毒家族是一种可以利用漏洞下载恶意代码的木马家族。该家族以 JS 脚本编写，攻击者可以下载恶意代码到感染者计算机中，窃取计算机信息。（威胁等级中）
		RiskWare[Monitor]/Win32.SpectorPro	该病毒家族是一种可以下载并安装推广应用的风险软件家族。该家族会修改系统配置文件，关闭安全防护软件。该病毒家族通过感染 .exe 文件和电子邮件附件传播。（威胁等级中）
		Trojan/Win32.Mixil	该病毒家族是一种下其他恶意代码的木马类程序。该家族文件安装在系统文件夹中，替换掉原有的 dll 文件。该病毒家族会下载木马文件到计算机中。（威胁等级低）
		Trojan[Packed]/Win32.BDF	该病毒家族是一种加壳类木马程序。该病毒家族会感染计算机中的文档，下载恶意代码到感染者的计算机中，收集计算机信息并回传。（威胁等级中）

保护混合云环境——实现可见性、可控性和灵活性

Benazeer Daruwalla，Rob Young/ 文 安天技术公益翻译组 / 译

企业部署混合多云策略的做法已经司空见惯，这种部署导致数据比以往更加分散。企业不仅要考虑在本地、公有云、私有云或混合云环境中运行哪些服务；还要确定如何通过数据安全方案来保护此类动态工作负载。

在《2018 年全球云观点调查报告》中，IDC 对超过 5700 家公司进行了调查，发现 81%的公司正在使用或计划使用公有云，86%的公司正在使用或计划使用私有云。与前一年相比，这两组数据都增加了 30%以上。

到 2020 年，全球超过 90%的企业将实施多云策略。大多数使用公有云的企业也将部署私有云平台，采用混合云策略。

企业的数据库管理解决方案模型就反映了上述趋势。常见的模型包括：

• 在本地或私有数据中心部署数据库管理解决方案（传统模型）。目前，企业通常根据工作的重要性及其对业务的影响来实现其现代化，但传统模型仍然是一种主导模型。

• 在公有云“基础架构即服务”（IaaS）模型上部署传统数据库管理解决方案。例如，在 Amazon EC2 上部署 Oracle 数据库服务器。

• 采用由云提供商托管和完全管理的“数据库即服务”（DBaaS）解决方案。例如，订阅 Amazon RDS for MySQL 或 Azure SQL 数据库。

• 使用云本地架构部署数据库管理解决方案。这包括在容器化环境（如 Docker）中运行 MongoDB 等数据库。

• 以上模型的组合

实现云的可见性和可控性

安全和 IT 企业正在努力跟上云服务提供商的快节奏创新。与此同时，他们还要根据不断发展的合规性要求来保护其数据。因此，采用混合多云方法保护数据正在迅速成为各规模企业的关键需求。虽然这看上去很棘手，但如果新方法实施得当，就可以帮助企业实现积极的差异化。

在向混合云架构转变期间，数据保护的基本驱动因素和用例保持不变。合规性、隐私和数据安全分析仍然是最重要的驱动因素。

话虽如此，在本地部署、私有云部署和公有云部署的组合中扩展数据安全解决方案和最佳实践，会引入额外的复杂性，企业必须解决这个问题。

最常见的云数据安全漏洞通常围绕可见性和可控性。虽然云部署模型可以提高 IT 速度和业务灵活性，帮助企业利用云的弹性和可扩展性，但由于缺乏细粒度的可见性和可控性，它们也会带来新的数据安全挑战。这是因为，云架构在云提供商和用户之间采用共享责任模型。

例如，使用 IaaS 模型，云用户可以实现类似于在本地部署的数据安全措施。然后，用户可以通过可操作的策略执行严格的控制措施。另一方面，使用“软件即服务”（SaaS）模型，云用户对服务数据的管理具有有限的可见性和控制权——甚至根本没有可见性和控制权。他们不得不依赖云提供商提供的有限、一刀切的方法。这会极大地限制公司保护敏感数据所需的细粒度控制能力。

因此，无论选择何种架构，用户都要确保采用适当的数据保护措施。

安全措施要紧跟进出混合云的数据

混合云数据保护策略必须解决这些限制，即，基于行业最佳实践和监管标准，实施灵活且专用的数据安全措施。具体而言，该策略应满足以下要求：

1. 可见性

具有数据资源活动其适当级别的可见性和粒度，对于采取有目的性的行动是必要的。

2. 可控性

对所有可见性进行集中化管理，以便做出近乎实时、高效和有效的决策，满足合规性要求并识别数据安全风险。

3. 灵活性

该策略必须能够适应不断变化的云和 IT 环境。企业应避免捆绑一家云供应商，而是根据不断变化的技术和业务需求灵活选择云服务和数据安全解决方案。

只要实施得当，混合多云数据保护方案就可以解决上述挑战，帮助企业在选择本地、公有和 / 或私有云服务时保护关键数据。

原文名称	Secure Your Hybrid Cloud Environment With Visibility, Control and Flexibility
作者简介	Benazeer Daruwalla，Rob Young。Benazeer Daruwalla 是 IBM 执行网络安全顾问。
原文信息	2019 年 5 月 24 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/posts/secure-your-hybrid-cloud-environment-with-visibility-control-and-flexibility/
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。