安天周观察

主办：安天　2017 年 3 月 6 日（总第 78 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天获 ISCCC 信息安全风险评估（一级）服务资质

近日，安天获得由中国信息安全认证中心颁发的“ISCCC 信息安全风险评估（一级）服务资质认证证书”。信息安全风险评估服务资质分为三个级别，其中一级最高。

信息安全风险评估是信息安全保障的基础性工作和重要环节，贯穿于网络和信息系统建设运行的全过程。通过对信息系统提供风险评估服务，可以全面、系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全整改措施，及时有效地防范和消除信息安全风险。

经过 17 年的发展，凭借多年来在政府、央企、军工、金融、运营商以及互联网等行业的风险评估工作中积累的大量成功经验，安天的安全服务能力和技术实力已经得到相关主管机构和重要客户的认可，并已形成了一整套规范且行之有效的信息安全风险评估服务体系。该资质的获得，进一步完善了安天的安全资质体系，也标志着安天能够为客户提供更高标准的安全服务。

安天为水利部提供全网安全服务解决方案

中华人民共和国水利部直接隶属于国务院，全面负责我国水利工作。水利部通过信息化网络办公，极大提升了工作效率，但同时也面临网络攻击风险。

为应对网络威胁，水利部已部署基础安全防护设备，为进一步提升水利部对抗网络威胁的能力，水利部需要在现有的安全防护设备基础上，增加专业的安全服务，实现以下目标：水利部全网的网络安全监测；水利部安全事件的分析处置以及应急响应；水利部安全策略的及时调整以及安全加固。

安天结合水利部的全网安全状况，为水利部提供专业的全网安全服务解决方案：

1）在水利部已有安全设备的基础上，部署安天探海威胁检测系统和安天追影威胁分析系统，进行威胁检测以及威胁捕获，构成威胁感知、捕获及追溯体系的数据基础；

2）通过全面监测水利部网络，及时发现攻击行为、重大安全事件以及安全隐患，定期提交分析报告以及合理化安全加固建议；

3）对发现的安全事件进行深度分析并提供高质量的分析报告以及处置建议；

4）对重大网络安全事件提供应急响应服务。

依托安天的安全服务解决方案，水利部目前已建立反 APT 攻击模型，具备应对 APT 攻击的能力；在建立应急响应体系基础之上，完善了重要信息系统及重点网站的安全监测、预警、应急处置管理机制，同时具备流量威胁感知、终端威胁感知和攻击载荷深度分析的能力，达到应对威胁能够快速响应，及时止损，实现了威胁与隐患统一发现、提早预警、快速处置的目标；另一方面也降低了水利部安全运维成本以及安全培训成本。

■ 亚马逊 AWS 出现故障　多家互联网服务受影响

近日，亚马逊云计算服务出现了较高的错误率，影响了数千个在线服务，包括项目管理工具和费用报告工具等。昨晚受到影响的网站服务有 Airbnb、Netflix、Slack、Spotify 等。亚马逊 AWS 报告称，S3 服务出现了“高错误率”。亚马逊将 S3 定位为“简单存储解决方案”，可用于储存数据，管理网络应用，以及提供用户可通过互联网下载的软件。根据 SimilarTech.com 的数据，S3 被近 15 万家网站使用，包括 ESPN 和 AOL 等。（来源：http://www.cnnvd.org.cn/news/show/id/8215）

■ 黑客可利用机器人安全缺陷或被用于攻击主人

近日，安全专家表示，世界上最著名的一些机器人存在监听它们的用户、泄露商业机密，甚至被控制、被用于实施身体攻击的风险。这些专家们警告，机器人很容易遭到网络攻击。网络安全公司 IOActive 测试了 50 台机器人，包括软银机器人 (SoftBank Robotics) 生产的孩子模样的 Pepper，以及 Rethink Robotics 的工业机器人 Baxter，结果发现了一些缺陷，黑客可以利用这些缺陷来操纵机器人的手臂和腿，或者控制麦克风和摄像头。（来源：http://www.cnnvd.org.cn/news/show/id/8220）

安天为新华社、北京市公安局、天津市公安局等单位提供安保服务

近期，为保障两会期间新华社的网络安全，安天安全服务团队协助新华社对网络进行全面安全评估和安全监测。

安天安全服务团队还协助北京市公安局、天津市公安局对两市部分重要市政服务系统进行了网络安保服务，在两会前完成了对部分重要网站系统和重要网络进行了安全检测，并在两会期间提供网络安全监测服务。

安天安全服务团队凭借多年来在网络安保、安全服务等工作中积累的大量成功经验，工作态度、技术能力得到相关主管机构和重要客户的高度认可。

每周安全事件

类 型	内 容
中文标题	谷歌 Project Zero 再曝微软 IE/Edge 浏览器安全漏洞
英文标题	Google Project Zero discloses another unpatched Microsoft Edge and IE Vulnerability
作者及单位	Pierluigi Paganini；SecurityAffairs
内容概述	近日，谷歌 Project Zero 公布了其在 Windows 10 中发现的一个漏洞，微软承诺将通过不久前的例行 Windows 安全补丁提供修补。而近期，Project Zero 团队再次对外公布了一项微软相关的安全漏洞，此次为 IE/Edge 浏览器相关的漏洞“CVE-2017-0037(CNNVD-201702-882)”，由该团队的 Ivan Fratric 发现，如果被黑客利用将可执行任意代码，Fratric 还公布了概念验证式破解演示。概念验证式破解中，Fratric 使用了 Windows Server 2012 R2 系统的 64 位 IE 版本，32 为 IE 以及微软 Edge 浏览器，表明这些浏览器均会被该漏洞影响。 据了解，Project Zero 在发现漏洞之后并不会马上公布于众，而是会将这一情况反应给软件开发商并给他们 90 天的修复时间，如果该开发商未在这一期限内完成修复那么团队就会对外公布。
链接地址	http://securityaffairs.co/wordpress/56716/hacking/cve-2017-0037-microsoft-flaw.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.chjiert.a[sys，exp] 2017-02-27	该程序安装后无图标显示，后台私自释放 su 文件获取 root 权限，修改其他系统文件读写权限，删除指定文件及路径，私自连网上传下载文件和数据。会给用户体验造成严重影响，存在较大风险，建议立即卸载。（威胁等级高）
		Trojan/Android.connector.a[exp] 2017-03-01	该应用运行后连网下载运行未知 DEX 文件，可能调用应用本身的下载、获取 root 权限、短信拦截等功能，影响用户使用，可能造成资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.djhero.a[prv，exp] 2017-03-01	该应用伪装成 Google 插件，运行后诱导用户输入手机号码，激活设备管理器，隐藏图标。后台上传用户手机号码、联系人和地理位置等信息，后台推送指定网站的内容，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.bigbustown.a[prv，exp] 2017-03-02	该应用伪装成正常应用，运行后会隐藏图标，接收远程指令，完成激活设备管理器，设置锁屏。监测手机进程，上传相关银行应用统计信息，推送虚假银行通知栏信息。会造成用户隐私泄露和资费损耗，以及造成用户经济损失，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.Triada.ac[exp]	该程序包含危险代码，运行后动态加载恶意子包，警惕该程序私自下载或私发短信造成用户资费损耗。（威胁等级高）
		Trojan/Android.privacySteal.d[prv]	该应用运行后收集并且上传用户的浏览器书签、用户短信、通话记录。监听来电和去电的号码，私自挂断电话。造成用户隐私泄露，建议立刻卸载。（威胁等级中）
		G-Ware/Android.Fakegupdt.cu[exp，rog]	该程序运行后会动态加载恶意子包，后台进行推送广告，私自下载安装未知应用，造成用户资费损耗，建议卸载。（威胁等级低）
		Tool/Android.CmcApp.a[prv，spy，rmt]	该程序是一款间谍工具，通过短信或网络控制设备，具有备份短信、通讯录、通话记录、网页历史信息和远程定位、阻止所有呼入 / 呼出电话等恶意行为，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。（威胁等级低）
		G-Ware/Android.jianmo.bx[rog，sys]	该应用伪装成正常应用，运行后会获取 root 权限，加载子包，置顶界面，勒索用户添加指定 QQ 进行付费解锁，造成用户资费损失，建议不要安装。（威胁等级低）
		Trojan/Android.Thief.b[prv，exp]	该程序为间谍应用，安装后无图标无界面显示，会执行接收短信指令，拨打电话、上传位置信息、发送设置信息到指定号码等高危行为，建议卸载避免隐私泄露和资费损耗。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Node.js 反序列化远程代码执行漏洞 CVE-2017-5941	Node.js 存在反序列化远程代码执行漏洞，Node.js 的 node-serialize 库中存在一个漏洞，该漏洞通过传输 JavaScript IIFE，利用恶意代码（未信任数据）达到反序列化远程任意代码执行的效果。并且 Node.js 服务端必须存在接收序列化的数据接口。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Radam	此威胁是一类可以加密用户文件并勒索赎金的木马家族。该家族样本运行后会加密用户文档并要求付费，有一定威胁。（威胁等级高）
		Trojan[Downloader]/Win32.Speccom	此威胁是一类可以连接网络下载恶意代码的木马家族。该家族样本运行后可以连接网络下载恶意代码并运行，还可以回传系统信息，有一定威胁。（威胁等级中）
		Trojan/Win32.Brambul	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后添加服务“Rvcrosoft Windows Genuine Updater.”，使用简单密码爆破，可以远程下发指令，窃取信息。（威胁等级中）

IaaS：云安全的下一篇章

Kaushik Narayan / 文　安天公益翻译小组 / 译

采用 IaaS 的企业必须使用共享责任模型来更新其安全方法

从制造业，金融服务到公共部门的各行业的公司信任云提供商，依靠他们的服务存储关键数据。SaaS(软件即服务) 应用程序 (如 Office365 和 Salesforce) 的快速增长就依赖于这种信任关系。SaaS 得以广泛应用是在 IT 专家确信云提供商可以提供与传统软件相当或更好的安全性。现在，第二波云应用浪潮正在迅速蔓延，企业将会融入 IaaS(基础架构即服务) 产品。要想更好地应用 IaaS，企业必须使用共享责任模型来更新其安全方法。

更新 IaaS 的共享责任模型

公司使用 SaaS 工具可以实现不同的功能：Office 365 用于协作，Workday 用于人力资源配置，Salesforce 用于客户关系管理。每个企业都为员工、客户和合作伙伴开发了内部应用程序，数量从几个到数千个不等。企业正在消除其数据中心，并将这些专有应用程序大量迁移到 IaaS 云产品中，所以使 IaaS 的增长速度是 SaaS 的两倍。

SaaS 和 IaaS 平台在不同的共享责任模式下运行，在云提供商和客户之间分配不同的安全能力。许多本应由 SaaS 提供商处理的安全漏洞会由这些托管于 IaaS 平台上的应用程序企业客户承担。

此外，因为企业面临快速迁移的压力，可能会导致开发团队没有额外的资源来更新预定迁移到云的内部应用程序的安全功能。专有应用程序没有 SaaS 应用程序那样的专有安全解决方案，也没有与安全产品集成的 API。过去，我们认为创业公司和云服务提供商负责保护 AWS，Azure 或 Google Cloud Platform 的安全。但是今天，世界 2000 强公司也会面临着受云端保护应用程序的挑战。

IaaS 安全威胁来自企业内部和外部。黑客攻击企业 IaaS 账户以窃取数据或计算资源。一位研究人员在 GitHub 上发现了超过 1 万个 AWS 凭证。被黑客入侵的账户可以用于挖掘比特币或勒索赎金。在企业内部，人为错误和疏忽会将公司数据和资源暴露给攻击者。医疗保健公司 CareSet 发生了一个配置错误，导致黑客利用其 Google Cloud Platform 账户对其他目标发起了入侵攻击。几天后，该问题仍然没得到解决，于是 Google 暂时关闭了该公司的账户。企业不能想当然地认为 IaaS 环境是安全的。在上述的情况下，云服务提供商都无力为用户解决这些漏洞。

IaaS 安全行动计划

保护 IaaS 平台上的专有应用程序中的数据安全，不能仅依靠 SaaS 的安全措施，更要保护计算环境本身。保护 AWS、Google Cloud Platform、Microsoft Azure 或其他 IaaS 平台首先要进行配置审查。以下是保护 IaaS 平台的四个至关重要的措施：

1）多因素身份验证

对于存储着敏感企业信息的任何应用程序来说，公司应为 root 账户身份和访问管理用户启用多因素身份验证，以降低账户泄露的风险。

2）检查无限制访问

不必要地暴露 AWS 环境会增加各种攻击威胁，包括拒绝服务、中间人攻击、SQL 注入和数据窃取。检查对亚马逊机器映像，关系数据库服务和弹性计算云的无限制访问可以保护知识产权和敏感数据，以及防止服务中断。

3）删除非活动账户

非活动和未使用的账户会对 IaaS 环境造成不必要的风险。审查和删除非活动账户可以防止账户泄露和滥用。

4）安全监控

将计算迁移到云中，最大的担忧之一是失去可视性和取证问题。启用审查追踪 (如 AWS 的 CloudTrail 日志记录) 可以创建一个行为监控工具，用于监控威胁和取证调查。

在这四个措施中，安全监控是最复杂和最可靠的。机器学习工具可以被调整，以检测威胁信标。API 可以根据会话位置、过度活动或强制登录启用监控功能。表面上将应用程序迁移到云可能会失去控制。实际上使用主动的基于云的安全策略，IaaS 上的应用程序可以与企业内部程序一样安全，甚至更安全。

原文名称	IaaS: The Next Chapter In Cloud Security
作者简介	Kaushik Narayan，云安全公司 Skyhigh Networks 的联合创始人和首席技术官，负责 Skyhigh 的技术愿景和软件架构。
原文信息	2017 年 2 月 24 日发布于迈克菲实验室 原文地址 http://www.darkreading.com/cloud/iaas-the-next-chapter-in-cloud-security/a/d-id/1328202?
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。

安天发布《勒索软件 KillDisk 分析报告》

近日，安天追影小组发现一款恶意软件 KillDisk。在第 71 期《安天周观察》中，安天追影小组分析了恶意软件 TeleBots，而 KillDisk 正是其中一个用于数据擦除的组件。在最新变种中，KillDisk 和勒索软件一样对文件进行加密，并向被感染者索要巨额赎金，且原本仅针对 Windows 平台的 KillDisk，已发展出针对 Linux 平台的版本。

虽然恶意软件 KillDisk 在 Windows 和 Linux 两个平台下的勒索信息基本是一致的，包括高达 222 比特币（约 218，000 美元）的赎金、支付比特币的地址、联系邮件等信息。但两个平台下的样本在具体的技术实现上仍有所区别。

在加密方式上，Windows 平台下的恶意软件首先会通过 CryptGenRandom 函数生成 256 位的随机密钥，对目标文件进行 AES 加密，再对 256 位的对称密钥进行 1024 位的 RSA 算法加密。同时，为了防止对文件重复进行加密，该恶意软件会给已加密的文件加上后缀“DoN0t0uch7h!$CrYpteDfilE”表意为“Donot touch this crypted file”。

而在 Linux 平台下，恶意软件会遍历指定的 16 个子目录，并对其进行加密处理。加密时会针对每 4096 字节的文件块，采用三重 DES 算法进行加密，每一个文件都将采用不同的 64 位加密密钥。

除此之外，在 Linux 平台下 KillDisk 会修改 GRUB 引导记录，把勒索信息写在引导记录处。在重新启动之后，被感染的系统将无法正常启动。值得一提的是，该勒索软件的解密密钥既没有存储在受感染主机上，也没有保存在 C&C 服务器上。所以即使受害者向勒索者支付了高额的赎金，依旧无法恢复已被加密的数据。

在恶意软件，安天提醒广大网络用户，要提高自身的安全意识，及时更新操作系统和杀毒软件；对于重要的数据、文件，一定要及时备份；不要随意点击来源不明的邮件，不可轻易下载附件。以免受到勒索软件冲击时造成财产、资料的损失。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 鉴定器、数字证书鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据智能学习鉴定器将文件判定为木马程序。

文件名	68CF2070D8FB4963211CFA4F2DAA72E5
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	172 KB
MD5	68CF2070D8FB4963211CFA4F2DAA72E5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransomware]/Win32.KillDisk
判定依据	智能学习

根据动态行为（默认环境）得出该文件具有以下行为：

枚举进程、遍历磁盘、获取计算机名、监听 DNS 服务端口，疑似篡改 DNS 服务器、获取计算机内存信息、获取磁盘类型、疑似桌面控制（字符串扫描）。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
枚举进程	★	遍历磁盘	★★
获取计算机名	★	监听 DNS 服务端口，疑似篡改 DNS 服务器	★★
获取计算机内存信息	★★		
获取磁盘类型	★	疑似桌面控制（字符串扫描）	★

报告地址：https://antiy.pta.center/_lk/details.html?hash=68CF2070D8FB4963211CFA4F2DAA72E5

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、美国软件交叉索引（NSRL）鉴定器、可交换信息（EXIF）鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

文件名	B9748EC5A7A0E3BC3CA139083CA875B0
文件类型	BinExecute/Linux.ELF
大小	27 KB
MD5	B9748EC5A7A0E3BC3CA139083CA875B0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransomware]/Linux.KillDisk
判定依据	智能学习

最终依据智能学习鉴定器将文件判定为木马程序。

根据动态行为（默认环境）得出该文件具有以下行为：修改 GRUB 引导记录、遍历子目录。

◆ 其他行为

行为描述	危险等级
修改 GRUB 引导记录	★★★★

◆ 危险行为

行为描述	危险等级
遍历子目录	★★★★

报告地址：https://antiy.pta.center/_lk/details.html?hash=B9748EC5A7A0E3BC3CA139083CA875B0