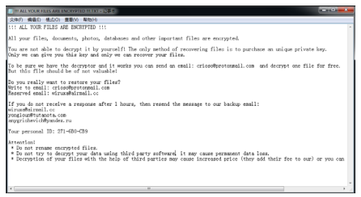
安天智甲有效阻断 Zeppelin 勒索软件

勒索软件名：	Zeppelin 勒索软件
传播方式：	垃圾邮件
加密算法：	AES+RSA
后缀：	.[User ID]
支付与金额：	通过邮箱与攻击者联系
免费解密工具：	暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Zeppelin 的勒索软件，该勒索软件最早发现于 2019 年 12 月，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序，该勒索软件程序执行后提示重新运行 svchost.exe 这一系统文件，确定后系统内的文件显示已经被加密。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 Zeppelin 勒索软件的加密行为。

Zeppelin 勒索软件样本运行后，提示 svchost.exe 系统文件存在异常，需重新运行，重新运行后桌面暂时变为黑色，短暂时间后桌面恢复正常并自动刷新一次，与此同时加密计算机上的部分文件，但不自动弹出勒索提醒和勒索信，在被加密文件原文件后追加以“.[User ID]”命名的后缀。在桌面和所有含有被加密文件的路径下创建名为“!!! ALL YOUR FILES ARE ENCRYPTED !!!”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 User_ID 等。



▲ Zeppelin 勒索信

Zeppelin 勒索软件采用“AES+RSA”加密算法，目前被加密的文件在未得到密钥前暂时无法解密。

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；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；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；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

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、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	Zeppelin.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	438KB
MD5	E26982B170856CA8CA96A2F41B2306FB
病毒类型	感染式恶意代码
恶意判定 / 病毒名称	Virus/Script.Generic
判定依据	关联分析

◆ 操作系统

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
文件篡改	★★★★★

◆常见行为

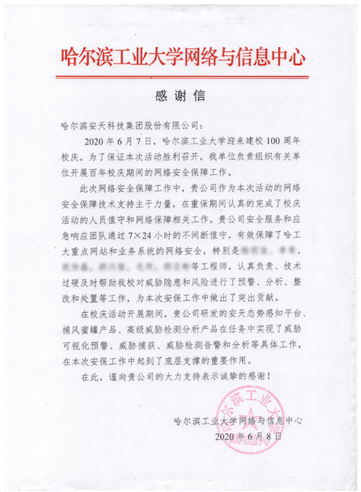
行为描述	危险等级
加载运行时 DLL	★
获取系统信息（处理器版本、处理器类型等）	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
获取驱动器类型	★
创建挂起进程	★★
设置调试器权限	★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 9 月 7 日 (总第 246 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天圆满完成哈工大百年校庆网络安保工作获高度认可

近日，安天收到哈尔滨工业大学网络与信息中心发来的感谢信，对安天在哈工大百年校庆期间所做的网络安全保障工作表示认可和感谢。信中表示，安天安全服务和应急响应团队在重保期间认真负责、技术过硬，在本次安保工作中做出了突出贡献；安天态势感知平台、捕风蜜罐系统、探海威胁检测系统、追影威胁分析系统在本次安保工作中起到了底层支撑的重要作用。庚子仲夏，筑梦百年。2020 年 6 月 7 日，哈尔滨工业大学举行了隆重的建校 100 周年校庆系列活动。为有效应对哈工大百年校庆活动期间可能发生的重大网络安全事件，最快速度地发现并处置病毒、木马、蠕虫等事件，安天为哈工大组建了应急响应团队，进行 7x24 小时不间断安全值守，并提供了威胁可视化、恶意程序监测预警、高级持续性威胁（APT）监测预警、威胁事件深度分析、威胁诱捕预警等功能，对发现安全威胁及时进行应急处置、取证与追踪溯源，为校庆活动顺利开展提供有力的网络安全保障。



哈尔滨工业大学网络与信息中心

感 谢 信

哈尔滨安天科技集团股份有限公司：

2020 年 6 月 7 日，哈尔滨工业大学迎来建校 100 周年校庆。为了保证本次活动胜利召开，我单位负责组织有关单位开展百年校庆期间的网络安全保障工作。

此次网络安全保障工作中，贵公司作为本次活动的网络安全保障技术支持主干力量，在重保期间认真的完成了校庆活动的人员值守和网络保障相关工作，贵公司安全服务和应急响应团队通过 7×24 小时的不间断值守，有效保障了哈工大重点网站和业务系统的网络安全，特别是[redacted]等工程师，认真负责、技术过硬及时帮助我校对威胁隐患和风险进行了预警、分析、整改和处置等工作，为本次安保工作中做出了突出贡献。

在校庆活动开展期间，贵公司研发的安天态势感知平台、捕风蜜罐产品、高级威胁检测分析产品在任务中实现了威胁可视化预警、威胁捕获、威胁检测告警和分析等具体工作，在本次安保工作中起到了底层支撑的重要作用。

在此，谨向贵公司的大力支持表示诚挚的感谢！

哈尔滨工业大学网络与信息中心

2020 年 6 月 8 日

多年来，安天始终坚持自主先进的能力导向，参与了 2005 年后历次国家重大政治社会活动的安保工作，为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考、天问一号等提供安全保障，并多次获得杰出贡献奖、安保先进集体等称号。

作为扎根龙江的网络安全企业，安天非常荣幸能参与本次哈工大百年校庆的重保工作且圆满完成任务。今后，安天会继续发挥核心技术与能力优势，为客户创造有效安全价值、提供有效防护。

伊朗 APT 组织冒充记者诱骗用户点击恶意链接

来自伊朗的APT组织Charming Kitten采用了一种新方法，通过WhatsApp和LinkedIn冒充讲波斯语的记者，以欺骗受害者打开恶意链接，该链接将用户带到网上诱骗页面以窃取凭据。研究人员说，攻击目标是来自海法大学和特拉维夫大学的以色列学者以及美国政府雇员。根据Clearsky的分析，最新的攻击活动是在7月首次发现的。

（原文链接：https://threatpost.com/charming-kitten-whatsapp-linkedin-effort/158813/）

研究人员发现广告欺诈僵尸网络 TERRACOTTA

White Ops的安全研究人员发现并追踪了一个庞大的广告欺诈僵尸网络，该网络使用数十个Android应用程序假装向用户提供免费项目，以使该应用存在至少两周。在最活跃的时候，名为TERRACOTTA的僵尸网络拥有超过65000台被感染的设备，欺骗了5000多个应用，并产生了大约20亿次虚假点击请求。研究人员称，TERRACOTTA恶意软件向Android用户提供免费商品，包括鞋子、优惠券和音乐会门票，但用户从来没有收到过这些东西。一旦安装该应用程序并激活恶意软件，该恶意软件就会利用该设备产生广告，使其看起来是合法的Android应用程序中显示的广告。

（原文链接：https://hotforsecurity.bitdefender.com/blog/aggressive-adware-promised-free-stuff-to-android-users-just-to-stay-installed-24035.html）

思科警告称电信级路由器中的漏洞已被积极利用

思科(Cisco)周末警告称，威胁分子正试图利用在电信级路由器上运行的思科IOS XR软件中的一个高严重内存耗尽拒绝服务(DoS)漏洞。思科的IOS XR Network OS部署在多个路由器平台上，包括NCS 540和560、NCS 5500、8000和ASR 9000系列路由器。该漏洞跟踪为CVE-2020-3566，是由于互联网群组管理协议(IGMP)数据包的队列管理不足所致。攻击者可以利用此漏洞，向受影响的设备发送精心设计的IGMP流量。成功利用该漏洞可能使攻击者导致内存耗尽，从而使其他进程不稳定。思科尚未发布软件更新来解决这一被积极利用的安全漏洞，但该公司在周末发布的一份安全建议中提供了缓解措施。

（原文链接：https://www.bleepingcomputer.com/news/security/cisco-warns-of-actively-exploited-bugs-in-carrier-grade-routers/）

每周安全事件

类 型	内 容
中文标题	亚马逊 S3 存储桶暴露 5.4 万张澳大利亚驾照扫描信息
英文标题	Australian Driver's Licenses Exposed on S3 Bucket
作者及单位	Jeremy Kirk
内容概述	据一位安全研究人员称，在开放的亚马逊简单存储服务 (S3 存储桶) 中，有 5.4 万张澳大利亚驾照扫描照被曝光，但尚不清楚是否会通知受影响的人。这些数据是由负责 Security Discovery 的 Bob Diachenko 发现的。其中一些数据的屏幕快照表明，它可能是在 2018 年被扫描。此次曝光的数据包括 108,535 张新南威尔士州驾照正面和背面的扫描，扫描内容包括出生日期、实际地址和驾照号码。数据还包括 .jpg 或 .pdf 文件中称为“法定声明”的完整文档。
链接地址	https://www.databreachtoday.com/australian-drivers-licenses-exposed-on-s3-bucket-a-14918

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 Excel 安全漏洞（CVE-2020-1496）	高	当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理员用户权限登录，那么攻击者就可以控制受影响的系统。
	Microsoft Edge 安全漏洞（CVE-2020-1568）	高	当 Microsoft Edge PDF 阅读器不正确地处理内存中的对象时，会触发远程代码执行漏洞。该漏洞可能以一种使攻击者可以在当前用户的环境中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。
	Microsoft .NET Framework 安全漏洞（CVE-2020-1046）	高	当 Microsoft .NET Framework 处理输入时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。若要利用该漏洞，攻击者需要能够将特制文件上传到 Web 应用程序。
较为活跃样本家族	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族木马具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	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[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	Trojan/Win32.Alien	中	此威胁是一种可以窃取密码信息的木马类家族。该家族木马运行后会窃取用户账户信息，记录键盘击键信息并回传攻击者服务器。
	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[Banker]/Android.Gustuff	中	此威胁是安卓平台上的一种银行木马家族。该家族木马通过恶意简讯进行传播，存在窃取金融凭证、自动执行交易和进一步感染用户的其他联络人等行为。
	Trojan/Android.Hqwar	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

如何保护企业免受 DNS 劫持

文森特·安杰洛 / 文 安天技术公益翻译组 / 译

2019 年 8 月，网络安全研究人员透露，一个名为 Sea Turtle 的黑客组织攻击了中东和北非的 40 家电信公司、互联网服务提供商、域名注册商和政府机构。

Sea Turtle 劫持了上述地区的外交部、情报 / 军事机构和能源相关团体的域名。这样一来，他们就能拦截发送给受害者的所有互联网数据，包括电子邮件和网络流量。

2020 年 6 月，日本加密货币交易所 Coincheck 报告说，黑客成功访问了其域名注册商，并劫持了其域名 coincheck.com。之后，黑客联系 Coincheck 客户，要求他们验证账户信息，然后利用这些信息访问客户的账户并从中窃取资金。

这两起事件说明，域名系统（DNS）劫持威胁日益严重。

DNS 劫持：保护企业及其域名

当用户输入或点击域名时，他们通常认为是要访问特定网站。但是，如果网络犯罪分子成功劫持了 DNS，就会将用户带到一个完全不同且危险的网站。他们这样做是为了获取经济利益。通过 DNS 劫持，他们还能拦截电子邮件（以进行间谍活动）和收集凭证，最终发动网络攻击。

公司域名等一系列名称具有营销意义，因此公司非常重视这些名称。客户和潜在客户通常会将公司与其品牌产品、服务和企业形象相关联。

然而，绝大多数公司尚未采取基本的安全措施来保护其域名。举例来说，大多数公司使用零售级注册商而非企业级注册商。相比于零售级注册商，企业级注册商能够了解其客户，并向其提供卓越的技术控制、认证标准、运营流程、合规实践、持续的漏洞评估和渗透测试等。

切勿忽视 DNS 劫持风险

为什么企业会忽视域名和与 DNS 相关的风险？这是因为，他们采用隧道视觉方法来解决网络安全问题，通常只关注熟悉的安全挑战。这使他们无法制定涵盖所有攻击向量的整体性策略。正如 Bitdefender 安全分析师西尔维·斯塔希（Silviu Stahie）所说：“公司通常会关注常见威胁，这样能够增强其端点和网络。但是，攻击者可以执行其他类型的网络攻击，在不损害公司基础架构的情况下伤害公司。因此，公司必须像重视其他形式的网络安全一样重视域安全。”

攻击者不断开发新方法，以增强其攻击能力。一旦成功劫持了企业的 DNS，攻击者就能进入企业网络，执行网络钓鱼活动，以窃取凭证、进行监视或执行其他网络活动。

为了有效地应对此类威胁，企业应部署以下两种策略。

●部署深度防御策略

这并非一个“新的”或革命性的概念。但是，企业并未将深度防御应用到域名保护中——他们需要这样做。强大的深度防御方法需要协同执行多层策略，从而将安全域、DNS 和数字认证实践结合起来。这包括控制用户许可，为任何试图访问域或 DNS 系统的人员部署双因子身份鉴别、IP 验证和联合身份管理。

此外，强大的深度防御方法还要利用注册锁定，域名系统安全扩展（DNSSEC）和基于域的消息验证、报告和一致性（DMARC）。通过注册锁定，注册商会与域所有者确认所有要求的更改，以消除对域的未授权更改和潜在风险更改。

DNSSEC 使用加密和密钥，通过验证数据中的数字签名来识别和阻止恶意 DNS 数据——签名必须与存储在主 DNS 服务器中的签名匹配，才能继续下一步操作。DMARC 执行电子邮件身份鉴别——邮件发送者和接收者共享信息，以验证给定的消息来自合法的发送者。这样可以防止黑客劫持公司的电子邮件域，进行诈骗和网络钓鱼。

●创建域安全委员会

在黑客世界中，犯罪分子会定期在论坛上共享信息和资源以不断改变花招，从而领先于预期受害者。公司也要不断增强防御能力，以应对层出不穷的攻击。公司亟需建立域安全委员会，在该委员会中，公司的首席信息安全官（CISO）与其他高管合作，创建并持续监控域安全实践和规程。该委员会还应开发一组 KPI，以不断衡量进度。

首先，企业要将域安全纳入其风险组成部分，然后将这个重要的安全盲区纳入企业的风险讨论中。

之后，企业应基于多层深度防御方法设定目标和优先级，以改善域安全状况。这包括连续评估企业锁定的重要域的数量。此外，企业可以监控用户权限或提权的变化，供应商 DNS 和 SSL/TLS 风险状况，以及其他安全指标（这些指标能够显示不使用 DNSSEC 或电子邮件身份鉴别 [SPF、DKIM、DMARC] 的重要域的安全状况）。

最后，域安全委员会需要及时了解当前的数字威胁形势。他们可以通过监控新威胁并以威胁情报报告的形式通知高管，来做到这一点。攻击者不断寻找新方法，试图渗透企业网络来实现非法目的。域安全委员会应及时将新的威胁情况通知公司，并评估风险。

结论

从某种意义上说，公司不太关注域名保护是可以理解的。毕竟，攻击者会通过网络和设备攻击迅速入侵企业，要及时了解所有威胁是非常困难的。但是，域是黑客可以利用的“重要门户”。

幸运的是，企业领导者可以在实施最佳实践的同时利用现有的深度防御工具。此外，他们可以创建域安全委员会，以进一步增强防御能力。通过这些措施，域这个“门户”对攻击者来说就是关闭的——希望永远是关闭的。

原文名称	Safe domain: How to protect your enterprise from DNS hijacking
作者简介	文森特 · 安杰洛（Vincent D'Angelo）。文森特 · 安杰洛是 CSC 数字品牌服务部战略联盟全球总监。
原文信息	22020 年 9 月 1 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/09/01/how-to-protect-your-enterprise-from-dns-hijacking/
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。