安天发布《Yarraq 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Yarraq 的勒索软件，该勒索软件隶属于 Hakbit 勒索软件家族，于 2019 年 12 月被发现，主要通过钓鱼邮件进行传播，邮件附件中包含一个图标为 PDF, 文件名为“hidden-tear.exe”的勒索程序，邮件内容诱使用户运行该勒索程序。

Yarraq 勒索软件执行后，加密计算机上的可执行程序和文档文件，在原文件名后追加名为“.yarraq”的后缀，修改桌面背景为勒索提醒，在含有被加密文件的位置创建名为“READ_IT.txt”的勒索信，桌面背景的勒索提醒和勒索信内容包含勒索说明、2000 美金比特币的赎金金额、联系邮箱和 USER_ID 等，在操作系统所在磁盘路径下创建名为“Rand123”的文件夹，将勒索程序移动至该文件夹内并修改名称为“local.exe”。Yarraq 勒索软件使用“AES+RSA”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。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口令；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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、字符串分析鉴定器、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、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	4cb4acca37fb90977f13b119779c5a76b4463db240c81efe1f7cff65039288c1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	214 KB
MD5	7269B1BA438915D5E54BA61DAA6FC6C5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/MSIL.Ryzerlo.A
判定依据	BD 静态分析

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
疑似窃取用户名或密码	★★★

◆常见行为

行为描述	危险等级
疑似桌面控制	★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	50399	224.0.0.252	5355
192.168.122.165	54669	224.0.0.252	5355
192.168.122.165	58500	224.0.0.252	5355
192.168.122.165	61269	224.0.0.252	5355
192.168.122.165	61272	239.255.255.250	1900
192.168.122.61	137	192.168.122.165	137
192.168.122.165	137	192.168.122.255	137
.....	.....	.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 1 月 6 日 (总第 215 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天蝉联中国网络安全技术对抗赛第一名

2019 年 7 月至 9 月，国家互联网应急中心（以下简称 CNCERT）在国家互联网信息办公室的指导下，举办了 2019 中国网络安全技术对抗赛（共 15 家企业参赛），本次大赛赛制发生变化，恶意代码分析引擎大赛和网络流量分析引擎大赛两赛合一。安天以嵌入下一代威胁检测引擎的追影、探海两项产品组合参赛并斩获第一名。去年，安天也包揽了该赛事两个项目的冠军。

CNCERT 举办的本次比赛面向国内网络安全企业，赛事组委会下设专家组、技术支持组对大赛考察内容、参赛答辩、成绩考核评判准则等进行评审。大赛提供真实的网络数据与业务场景，旨在全方面考察参赛产品的核心检测分析引擎的技术能力与业务实战能力。

探海威胁检测系统是安天针对政企网络出口、重要网段和互联网关口等场景研发的网络威胁旁路监测设备，其以网络流量为检测分析对象，实现对网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动、病毒扩散传播、木马远程控制等网络行为的检测和告警，能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁。探海可与安天威胁情报服务结合，对多个 APT 攻击组织的载荷工具和 C2 基础设施实现带有精确组织指向的报告告警。

追影威胁分析系统是安天面向高级威胁场景对象需求研发的文件深度分析设备，其以文档文件、可执行文件、URL 为分析对象，采用深度静态分析与沙箱动态加载执行的组合机理，借助包括安天下一代检测引擎在内的多组鉴定机制组合对输入对象进行判定分析，实现漏洞利用触发、细粒度揭示载荷行为，形成私有化的威胁情报生产能力。追影可有效检出分析鉴定各类已知与未知威胁，尤其对基于格式文档的 0day 漏洞攻击具备优秀的检出能力，通过动静态结合的手段对各种格式的文件进行细粒度的向量提取和解析，深度揭示威胁行为细节，输出详实报告。追影在进行判定后，结合白名单过滤机制，可以输出多种样式的威胁情报，实现客户私有化的情报生产能力，辅助威胁处置和威胁猎杀工作。追影与安天威胁情报服务结合，可以实现对载荷关联 APT 攻击组织的精准指向，并基于威胁框架评估载荷的能力模型。

探海和追影两款产品组合使用，可以同时发挥探海的高速检测优势和追影的检测深度优势。探海将还原到的恶意程序和可疑文件投放给追影分析，追影对相关对象做出二次检测判定，同时细粒度触发威胁行为，并将对象加载执行产生的 C2 等信息，以情报推送的方式回传给探海，形成联动效果。

安天下一代威胁检测引擎 AVL SDK 为安天全线产品提供了有力的赋能支持。面对威胁的演进变化，安天提出了下一代威胁检测引擎的理念，基于面向高级威胁、体系化攻击，单点安全环节均会被绕过的特点，安天将反病毒引擎从单一的检测识别单元，提升为封装检测识别、向量拆解、关联判断的复合安全中间件。通过全格式识别、全向量解析，使反病毒引擎不仅可以输出对海量威胁的精准识别结果，也为产品和态势感知平台体系输出基础静态向量数据以支撑分析研判、威胁关联追溯、客户自建深度普查和处置规则。

检测引擎是安天长期自主研发创新的核心基础能力，安天 AVL SDK 引擎曾先后获得科技部创新基金（2004）、国家 863（2006）和发改委信息安全专项（2008）、工信部工业互联网专项（2019）支持，AVL SDK 检测引擎的移动版本曾获得中国厂商首个 AV-TEST 年度奖项。安天以引擎授权模式，形成了产业协同生态。安天目前已累计为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。这进一步扩展了安天全面的威胁感知和威胁情报能力。

随着能力的全面发展提升，安天在“三高”（高信息价值、高防护等级、高威胁对抗）客户场景中逐渐担当起协助规划、整体赋能的主责，研发重心逐渐转入到实战化运行的战术型态势感知平台中。反病毒引擎已从安天的核心能力，转化为安天全线产品的基础支撑性技术；赛博超脑体系已从安天后端自动化分析体系，转化为安天威胁情报赋能平台。在支持全体系架构和各种操作系统的基础上，安天还针对各种国产环境优化了引擎版本。

在坚持引领恶意代码检测对抗优势技术能力的基础上，安天正在走出反恶意代码方法路径依赖，向全面体系化能力成长。自 2019 年 6 月 30 日，安天从引擎到主线的端点防护、流量监测、威胁分析产品均支持对威胁框架（双标支持 ATT&CK 和 Technical Cyber Threat Framework）知识标签的输出，并在态势感知平台中进行标签整合。引擎作为安天的核心能力，将会随着安天产品和态势感知体系在更多客户侧的落地，创造出更多的支撑价值。

微信扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	黑客利用纽约特奥会的服务器向捐赠者发送钓鱼邮件
英文标题	Nonprofit organization Special Olympics New York hacked and its server used to send phishing emails
作者及单位	Pierluigi Paganini
内容概述	纽约特奥会为智障人士提供了参加奥林匹克式的训练项目的机会。不幸的是，这家非营利组织在圣诞节期间遭到黑客攻击，攻击者随后利用其电子邮件服务器发起了针对捐赠者的网络钓鱼活动。该组织披露了此次黑客攻击，并宣布已锁定攻击者，还向受影响的人发送了数据泄露通知，建议他们无视该组织最后收到的信息。
链接地址	https://securityaffairs.co/wordpress/95796/data-breach/special-olympics-new-york-hacked.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 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

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.SwordSpy.a[prv,rmt,exp] 2019-12-28	高	该应用程序私自窃取用户的通话记录、通讯录、短信记录、设备固件等信息，私自对通话进行录音，未经允许发送短信，联网上传指定数据或文件到服务器并获取远程指令，根据指令执行相应行为，这些行为会造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.Youzicheng.a[exp,rog] 2019-12-29	中	该应用程序伪装邮件应用，运行隐藏图标，后台私自下载安装代理相关文件并提权，可能用于内网渗透，存在较大风险，建议卸载。
		G-Ware/Android.ApkolToot.a[rog,exp,fra] 2019-12-30	低	该应用程序伪装色情应用，本身无实际功能，加载广告，私自提权，下载、静默安装未知应用，造成用户资费消耗，建议不要使用。
	较为活跃样本	Trojan/Android.SmsSpy.cr[prv,exp]	中	该应用程序运行获取用户短信并转发至指定网址，造成用户的隐私泄露，建议卸载。
		Trojan/Android.ElitSevda.a[prv,spy]	中	该应用程序运行获取用户设备信息，监听用户通话并录音，监听用户短信，并通过邮件上传，造成用户隐私泄露，请立即卸载。
		Trojan/Android.Youzicheng.c[prv,rog]	中	该应用程序运行隐藏图标，窃取用户 facebook、chrome 等应用的 cookie 并上传，造成用户隐私泄露，建议卸载。
		Trojan/Android.SmsSend.pw[exp]	低	该应用程序伪装成正常应用，私自调用发送短信，可能会造成资费消耗，建议卸载。
		G-Ware/Android.Dowgin.i[rog,exp]	低	该应用程序被恶意重打包捆绑流氓广告插件，弹出广告并诱导下载应用，造成用户流量消耗，存在流氓行为，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft PowerPoint 远程代码执行漏洞（CVE-2019-1462）	高	当 Microsoft PowerPoint 软件无法正确处理内存中的对象时，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用户权限登录，攻击者便可控制受影响的系统，随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan/Win32.Inject	中	此威胁是一种木马类程序。该家族将自身以某种方式注入到其它进程中（避免用户和杀毒软件感知、清除），隐藏自身，并在后台执行恶意行为。因此该病毒家族是一种通过行为来命名、定性的木马类程序。
		Trojan/Win32.StartPage	中	此威胁是一种木马类程序。该家族会将浏览器首页地址修改为指定地址，这些地址通常是广告页地址。该家族的有些变种会将浏览器首页地址修改为挂马网站或钓鱼网站地址；还有部分变种会修改系统 host 文件，使用户无法正常访问安全网站。
		Trojan[PSW]/Win32.Fareit	中	此威胁是一种盗取用户账户密码等信息的木马类程序。该家族木马入侵用户系统后，会盗取用户的账户密码等信息。部分家族变种会在被感染的电脑中安装可以采掘比特币的“CGMiner”软件，并将采掘到的比特币并发送给黑客。
		GrayWare[AdWare]/Win32.DomaIQ	低	此威胁是一种广告类的灰色软件程序。感染该家族后，用户会在网页上看到广告信息，如搜索商品、弹出式广告、插播广告、文字链接广告等。该病毒被分布到 IE、谷歌、火狐等浏览器插件及金融平台中。该家族感染浏览器后会修改浏览器设置（如：主页、搜索设置等）；有些变种还会修改 IE 浏览器的加载时间阈值，并将火狐浏览器装入锁文件，以阻止其他软件修改浏览器设置等。
		GrayWare[AdWare]/Win32.Lollipop	低	此威胁是一种灰色软件。该家族运行后，会在用户浏览网页时弹出广告，还可以重定向用户的搜索结果、监测用户行为、在系统中下载应用程序并运行，并将用户信息发送给黑客。该家族通常放置在程序网站上，或与一些第三方软件的安装程序捆绑在一起。

2020 年 CISO 的六个目标

Joan Goodchild/ 文 安天技术公益翻译组 / 译

又到了年末，安全领导者是时候评估 2019 年的工作成就并确定 2020 年的优先事项了。

首先，我们回顾一下 2019 年的情况。研究发现，尽管企业增加了安全投资，但是数据泄露事件持续增加。每起事件造成的平均损失达到 392 万美元，比 2018 年增加了 1.5%。Enterprise Strategy Group 预测，今年 58%的企业将增加网络安全支出。

新年在即，企业是时候揭开安全工作的新篇章，引领安全策略朝着崭新的方向发展了。也许，你想在明年推出新的工具或策略，或整合新的思想和流程。也许，你只是希望安全团队能够更有效地工作。

我们采访了多位首席信息安全官（CISO），询问他们 2020 年的计划。以下是他们的一些主要目标。

使安全成为业务驱动力

“企业经常因为信息安全的原因不敢去做某事，或者更糟糕的是，因为信息安全的原因抑制一些能够推动业务向前发展的想法。”PAS Global 公司的 CISO 杰森 · 哈沃德 · 格劳（Jason Haward-Grau）表示，“在 2020 年，我们应该将安全赋能过程嵌入到业务中，确保信息安全完全嵌入到业务价值链中。”

Digital Shadows 公司首席信息官兼战略副总裁里克·霍兰德（Rick Holland）表示：“在 2020 年，CISO 应该更好地了解其业务如何增加企业收入并最大程度地降低成本。”

优先考虑隐私问题

Crypto.com 的 CISO 杰森 · 刘（Jason Lau）表示：“2020 年，我计划制定围绕信息隐私的新策略，制定全局隐私计划。”他表示，将以最近发布的 ISO 27701 和即将发布的 NIST 隐私框架作为指南。

“当前，所有行业都缺乏隐私意识。”他说。“我的目标不仅是提高员工的数据隐私意识，还要将数据隐私嵌入到企业的不同流程中。我认为，企业应尽早评估产品的安全性和隐私影响，在产品设计时充分考虑隐私问题。这对于所有企业都是至关重要的，有助于保护隐私。”

关注安全的“人为”方面

“在 2020 年，我计划投入更多的时间来审查和改进信息安全条款的‘人为’方面，确定薄弱环节、策略缺陷和缺失协议——这些都有可能损害我们的整体保护网。”English Blinds 公司 CSO 艾莉森 · 戴维斯（Alison Davies）说。“这些方面包括：高层员工随地存放公司笔记本电脑、包含专有技术的建筑物和区域的访问协议不严谨，或者彼此熟悉的员工为了方便起见共享访问密码等。”

关注敏捷性

“将安全性集成到敏捷流程中，意味着在软件开发周期之初就将安全性考虑在内。这样做可以带来很多好处，包括增强创新能力、与其他团队协作，以及对产品的安全性更有信心等。但是，在敏捷性方面，某些安全的计划可能比其他团队更加成熟。

Cybereason 公司 CISO 伊斯雷尔 · 巴拉克（Israel Barak）表示：“在 2020 年，我计划为安全团队引入更多的敏捷流程以及日常运营能力，这将有助于减少冗余和自满。我希望，通过更好地实现重复程序的自动化，帮助每个人提高技能，最终改善企业的安全决策。借助更好的决策并减少自满情绪，员工能够提高工作效率。”

对数据和系统更好的可见性

“容器化、微服务和分布式计算的整体进步，提供了令人难以置信的弹性和增长能力。”Unity Technologies 公司安全总监安德烈亚斯 · 豪格尼斯（Andreas Haugsnes）指出。但是，如今有太多的内容需要控制和管理，因此这些进步带来业务创新的同时，也带来了安全问题。

因此，豪格尼斯希望在 2020 年获得更好的可见性。

他说：“我们面临更大的挑战——即在任何时间映射数据保存、流动或计算的位置。鉴于安全环境不断变化，我希望获得对数据更好的可见性和控制，并在可能的情况下进行嵌入。”

YL Ventures 公司 CISO 罗杰 · 黑尔（Roger Hale）也提出了可见性目标。

“我们生活在一个无边界的生态系统中，我们的员工在其中工作，并创建和使用数据。”他说。“我计划采用‘数据访问优先’的方法。现在，我们处在一个以数据为中心的互联世界中，通过跟踪对数据的访问以及谁在对数据进行操作以及移动数据，我们可以构建跨本地、云端和移动端的数据映射。”

使安全工作变得有趣

鉴于安全行业存在严重的技能差距，2020 年企业应努力吸引人才。企业应该思考，除了实际工作之外，应该如何吸引有才能的安全专家为其效力。

“我认为企业需要招募‘首席娱乐官’或将该工作内容添加到每位高管的职责中，包括信息安全高管。”PAS Global 公司的哈沃德 · 格劳（Haward-Grau）说。“在过去的 15 年中，我一直致力于证明‘让工作变得有趣’这一价值观。但是在挑战或危机时期（尤其是在信息安全领域），我们会很快忘记这一点。明天的安全情况不会比今天乐观，因此我们最好现在就行动起来。安全工作应该是令人愉快的，而不是令人烦恼的。”

原文名称	6 CISO New Year's Resolutions for 2020
作者简介	Joan Goodchild。Joan Goodchild 是一位资深记者和编辑。
原文信息	22019 年 12 月 30 日发布于 Dark Reading 原文地址 https://www.darkreading.com/theedge/6-ciso-new-years-resolutions-for-2020/b/d-id/1336690
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。