安天发布《Deniz_ Kızı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“Deniz_Kızı”的勒索软件，该勒索软件隶属于 Keslan 勒索软件家族，此家族最早于 2019 年 12 月被发现，主要通过垃圾邮件传播，邮件附件中包含一个名为“svchost.exe”（Windows 服务主进程）的勒索程序，目的是伪装成 Windows 系统中的程序，诱使用户运行该勒索程序。

“Deniz_Kızı”勒索软件运行后，加密计算机上的文档文件，在原文件名后追加名为“.Deniz_Kızı”的后缀。此后缀为土耳其语的两个单词，译为“美人鱼”，并在桌面文件夹、库文件夹和系统根目录下生成名为“Please Read Me!!!.hta”的勒索信，加密结束后，弹出一个勒索提示窗口，同时打开勒索信，该勒索信内容包含勒索说明、邮箱联系地址、价值 400 美金比特币的赎金金额、购买比特币的教程和两个 USER_ID 等。“Deniz_Kızı”勒索软件使用“RSA+AES”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、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、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、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	deniz_kizi.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.23 MB
MD5	583212EB42CE3662B399693BBB7D5FD2
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Graftor
判定依据	BD 静态分析

◆ 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
禁用权限管理（UAC）	★★★
检测虚拟机	★★★★★
延时	★★★

◆常见行为

行为描述	危险等级
壳行为填充导入表	★★
加载运行时 DLL	★
获取系统版本	★
获取计算机名	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
检测自身是否被调试	★★
镜像劫持	★★
检索系统内存信息	★
创建窗口	★
启动指定服务	★
.....	.....

◆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 13 日 (总第 216 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

威胁框架：价值的认知—安天冬训营首日纪实

2020 年 1 月 8 日，由中共黑龙江省委网络安全和信息化委员会办公室、黑龙江省科学技术厅、黑龙江省公安厅主办，中国信息安全测评中心提供技术指导，哈尔滨市松北区人民政府、安天科技集团股份有限公司、中国网络安全产业联盟、黑龙江省科力高科技产业投资有限公司承办的网络空间威胁对抗与态势感知研讨会暨第七届安天网络安全冬训营在哈尔滨开幕。

本届冬训营为期两天，以“寒夜远征”为营语，以“威胁框架: 认知与实践”为主题。业内专家与安天工程师一同深入分析，分享和共商对威胁框架安全价值的理解和实践思考。我们围绕用户的关切，分析来自不同层级威胁行为体的攻击事件，介绍在检测引擎、端点防护、流量监测、深度分析、态势感知等方面威胁框架的结合进展，及在重要信息系统和关键基础设施中建立有效防御体系的探索实践。

在首日的开幕式上，黑龙江省委网信办副主任王希忠发表了致辞。他表示，当前我国网络安全形势依然严峻，防护能力较为薄弱，难以对抗国家级、有组织的高强度网络攻击。以安天为代表的网络安全企业，承担着维护和保障国家网络安全的责任和使命，是国内与威胁对抗的主要力量。

会上，主持人陈晓桦向来宾分发了由安天 CERT 编写的《2019 网络安全威胁年报》（征求意见稿），希望现场嘉宾能够对安天的工作提出宝贵的意见和建议。

2020 年安天第七届网络安全冬训营主旨报告

安天负责人肖新光发表了《从反恶意代码小闭环到威胁对抗大闭环》的主旨报告。报告详述了安天自 2000 年起在威胁检测引擎、大规模自动化分析体系、恶意代码捕获分析以及端点、流量等环节上所进行的基础能力建设的探索过程。

该报告还分享了安天在尝试从单纯的反恶意代码视角提升至威胁对抗视角时遭遇的多次挫折和取得的经验教训，并由此提出了安天引入威胁框架作为自身新一轮能力建设导向的考虑。过去的一年里，安天团队在业内专家的指导下，围绕威胁框架，根据实际情况完善了各产品能力。报告中还展示了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、捕风威胁捕获系统、拓痕安全工具等相关产品在威胁框架视角下的能力图谱映射，表达了安天希望从传统的反恶意代码小闭环切换到赋能客户、共建防御加威胁对抗大闭环的决心。

安天工程师分享网空威胁框架的演进

安天解决方案中心工程师在会上发表了《网空威胁框架的演进》的报告。报告指出：在当前网空对抗形势下，威胁框架是认知威胁的重要方法，也是安全厂商提高客户安全防御能力、达成客户安全价值的有效途径。当前，网空威胁主要是 APT 形式的攻击，要求我们改变以往所采用的离散化的威胁分析方法，基于攻击者视角，以整个攻击行动来统一离散的威胁事件，形成对威胁的整体性分析，从而获得更为有效、更有防御价值的分析结果。威胁框架的核心价值在于分析防御差距、检测 / 缓解攻击者着重使用的技术、跟踪特定对手的技术集合、指导攻击者模拟、评价安全技术，优化安全部署、分析攻击行为与威胁发展态势等几个方面。

该报告依次介绍了洛克希德 . 马丁杀伤链框架、ATT&CK 威胁框架、ODNI 公共网空威胁框架、TCTF 威胁框架的相关情况，并通过对比说明了 ATT&CK 威胁框架和 TCTF 威胁框架协同作用和互补效果。

安天向所有来宾分发了用于介绍威胁框架的核心价值的 ATT&CK 威胁框架挂图（安天翻译版本）。

业内专家从云安全角度感知网络空间安全的新威胁

南开大学网络空间安全学院教授张健在会上发表了《从云安全感知网络空间安全的新威胁》的主题演讲，探讨了如何运用 ATT&CK 威胁框架中云计算相关内容，分析云计算所面临的威胁状况。

他表示，在 AI、大数据、5G 等新技术新应用推动下，云计算技术快速发展，全球云计算市场将迎来爆发式增长。与此同时，云安全问题也日益凸显，根据 CNCERT 的报告，云计算平台不仅成为黑客攻击的主要目标，同时也成为攻击的源头。这是由于政府、企业等单位越来越多的应用和数据逐步迁移到云平台，云平台承载着高价值的数据资产，成为黑客攻击重点。另一方面由于云计算技术自身的不足，从硬件、虚拟化、网络层到应用层等各个层面存在安全漏洞，云内部安全管理和防护机制也不尽完善，云平台受到内外部攻击被黑客控制和利用成为攻击源，严重危害网络和云平台的安全。特别是随着政府和关键信息基础设施运营单位大量使用云平台，我们面临的安全威胁发生了显著变化。我们要准确把握和应对新变化和新威胁，要加强对云安全技术的研究和开发，吸引更多的企业提供优质的安全云产品和服务，建立形成良好的云安全生态。同时加强关键信息基础设施的保护，开展态势感知研判，提升对安全威胁的发现和预警能力。

最后，安天研究院分享了《美军武器系统风险管理的认知与启示》。

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	Lazarus 开展针对加密货币的后续 AppleJeus 行动
英文标题	Operation AppleJeus Sequel Lazarus continues to attack the cryptocurrency business with enhanced capabilities
作者及单位	GReAT
内容概述	卡巴斯基研究人员发现了 Lazarus 组织针对加密货币领域的后续 AppleJeus 行动。在该后续活动中，Lazarus 开发了自定义 macOS 恶意软件，其使用 Object-C 框架，托管在 GitHub 上，并添加了一种身份验证机制，在不接触磁盘的情况下加载下一阶段有效载荷。针对 Windows 用户目标时，Lazarus 建立了 wfcwallet 的虚假网站，并制定了多阶段感染程序，感染始于 .NET 恶意软件，其伪装成 WFC 钱包更新程序，执行后，将模仿连接到 C2 地址的钱包更新程序。然后，攻击者使用 RasMan Windows 服务通过持久性机制下载有效载荷。研究人员目前发现了在英国、波兰、俄罗斯和中国的几名受害者，大多都与加密货币业务实体有关。
链接地址	https://securelist.com/operation-applejeus-sequel/95596/

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.oscleanerspy.a[prv,rmt,spy] 2020-01-05	高	该应用程序注入恶意代码，运行获取远程指令，窃取用户设备信息，短信，通讯录，通话记录，社交软件信息等敏感信息并上传至服务器，造成用户隐私泄露，建议卸载。
		Trojan/Android.emial.hb[prv,exp,rog] 2020-01-06	中	该应用程序运行后激活设备管理器，防止用户卸载，同时私自窃取短信记录、通讯录、手机固件信息，发送到指定邮箱和手机号，会造成用户隐私泄露和资费消耗，建议立即卸载。
		Ware/Android.soraka.a[exp,rog] 2020-01-07	低	送流氓广告，造成用户资费损耗，建议卸载。
	较为活跃样本	Trojan/Android.smkl11.d[prv,spy]	中	该应用程序伪装为系统软件，运行隐藏图标，会上传用户的短信信息、通话记录、位置信息等，造成用户的隐私泄露，建议卸载。
		RiskWare/Android.Daikuan.q[rog]	中	该应用程序运行后显示虚假贷款界面，访问其他第三方网贷网站，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。
		G-Ware/Android.LockScreen.cv[rog,lck]	中	该应用程序运行后隐藏图标，开机自动启动，锁定用户界面，影响手机正常使用，建议卸载。
		G-Ware/Android.HiddenAds.ka[exp,rog]	低	该应用程序包含风险代码，运行加载恶意子包，推送广告，静默下载，会造成用户资费损耗，建议卸载。
		G-Ware/Android.HiddenAds.kc[exp,rog]	低	该应用程序安装无图标，运行就加载子包，推送广告，造成用户资费损耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Hyper-V 远程代码执行漏洞（CVE-2019-1471）	高	当主机服务器上的 Windows Hyper-V 无法正确验证来宾操作系统上已通过身份验证的用户输入时，会触发远程代码执行漏洞。攻击者可以在来宾操作系统上运行经特殊设计的应用程序来利用此漏洞，从而执行任意代码。
	较为活跃样本	Trojan/Win32.Midhos	中	此威胁是一种木马类程序。该家族会在被感染电脑中下载恶意软件，为浏览器安装恶意扩展工具，导致搜索结果重定向。该家族将网站重定向为能使黑客获利的恶意网站，当用户访问了恶意网站，该家族便利用漏洞，在 Java 软件或 Adobe 软件中安装恶意文件，从而入侵用户电脑。
		Trojan[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马程序。该家族入侵电脑后，会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
		Trojan[Dropper]/Win32.Sysn	中	此威胁是一种带有捆绑功能的木马类程序。该家族样本感染用户系统之后，会在电脑中释放并安装其它恶意程序。部分变种还可以对电脑进行远程控制，关闭电脑中的杀毒软件。
		GrayWare[AdWare]/Win32.InstallMonster	低	此威胁是一种广告类程序。该家族会在电脑中安装并运行广告件程序，还会窃取用户的上网行为方式等敏感信息。
		GrayWare[AdWare]/Win32.BrainInst	低	此威胁是一种具有广告行为的木马类程序。该家族样本运行后会在电脑中下载并安装多个程序，如 IE 工具栏，推广软件等程序。

2020 年七大网络趋势

安德鲁·弗洛里希 / 文 安天技术公益翻译组 / 译

在本文中，我们将介绍 2020 年将会出现的七大网络技术和架构趋势。

2020 年，企业 IT 将会非常忙碌。过去几年，除了在整个园区内实施 SD-WAN 和 WiFi 6 升级外，企业 IT 网络团队在实施新技术方面有些缓慢。但是到 2020 年，很多网络团队将采用先进的平台、工具和方法，将老化的网络带入一个新时代。在本文中，我们将介绍企业 IT 部门正在或应该在计划的项目。

从高层角度来看，网络团队的任务是创建支持新兴服务的网络，提高工作效率并扩大公司网络的覆盖范围。先前手动流程的数字化，将推动对更快的网络速度和新服务的需求。很多技术将在 LAN/WAN 中实现，而其他技术则更多地面向云和服务提供商。这些技术可以增强可见性和部署速度，最终大大提高企业的生产力。接下来，我们将介绍 2020 年将会出现的七大网络技术和架构趋势。

网络自动化

企业对快速部署网络服务的需求，开始超过其网络团队的能力。幸运的是，网络自动化工具应运而生。无论企业使用的是商业网络供应商的标准商业化产品，还是开源产品，都能够实现以下任务的自动化。

- 重复性的网络配置任务
- 配置验证测试
- 重复部署
- 重复性的运营管理任务

5G 连接分支机构

我们主要从移动设备连接的角度来看 5G。5G 技术很重要；从分支机构的角度来看，这种新的无线技术也将增强企业实力。从 2020 年开始，网络供应商开始将 5G 技术集成到其蜂窝分支机构网关中。这将帮助企业快速部署远程站点，数据速度可以与更昂贵的有线宽带替代方案相媲美。对于需要能够快速启动或转移办公室的企业来说，5G 将成为一项改变游戏规则的技术。

物联网（IoT）网络分段与监控

2020 年，IoT 将成为现实。由于 IoT 设备存在严重的安全问题，这些设备与网络其他部分的虚拟分段将成为网络部门的主要任务。建立安全区域（称为微分段）将使 IoT 设备可以在同一公司网络上运行；同时这些处于安全区域中的 IoT 设备，不会因为自身安全级别低，进而危害处于同一网络环境中的其他公司设备。

一旦实施分段，对 IoT 设备的监控很可能将由网络团队负责。端到端的 IoT 监控，不仅有助于提高性能，还可以确定 IoT 设备通信何时偏离正常状态，从而确保其不受感染。

互联网边缘的精简

随着企业将更多的应用程序、数据和服务迁移至公有云中，很多企业意识到，其数据中心几乎没有服务器运行面向互联网的服务。这意味着，当前的互联网边缘架构比企业所需要的更加复杂。

边界网关协议（BGP）通常用于互联网边缘，通过连接到具有相同公有 IP 空间的两个或多个 BGP 对等方来提供完整的互联网冗余。但是，如果所有面向互联网的服务都位于公有云中，企业的专用网络就不需要该级别的入站互联网冗余了。相反，企业仅需要出站互联网冗余。在这种情况下，企业可以在互联网边缘消除 BGP，采用更精简的出站互联网负载平衡技术。

网络分析

大数据和人工智能（AI）技术不断发展，已经达到了可以提供前所未有的网络性能状况信息的地步。2019 年，一些企业已经尝试在其环境中使用网络分析（NA）工具。此外，很多企业将从 2020 年开始在其生产环境中使用 NA 工具。

跨混合和多云网络实现一致的策略

从网络角度来看，企业在过去几年中最大的麻烦之一是：需要在多个云中创建并维护一致的网络和网络安全策略。由于公有和私有云数据中心使用不同的基础网络设备，因此创建策略的配置步骤通常大不相同。随着企业从混合云转移到多重云架构，在私有云和公有云网络之间维护一致的网络和安全策略的需求将势不可挡。

在 2020 年，多重云管理平台将成为解决此问题的一种方法。此外，许多云服务提供商已经开始为客户提供多重云策略管理工具。例如，AWS 最近发布了 AWS Outposts。Outposts 提供了一种在数据中心之间扩展 AWS 策略、服务和 API 的方法。因此，跨多个云管理一组网络 / 安全策略将不会像过去那样困难。

边缘计算改变一切

与传统的云计算相比，边缘计算旨在使计算和数据更接近最终用户。这样做显著降低了带宽成本，同时还降低了网络延迟。预计网络运营商将从 2020 年开始为客户提供边缘服务。尽管企业用例目前相对较少，但是在不久的将来，边缘计算几乎可以用于所有业务领域，帮助企业降低成本、改善流程，或创造竞争优势。

原文名称	7 Network Trends You Can Expect in 2020
作者简介	安德鲁·弗洛里希（Andrew Froehlich）。安德鲁·弗洛里希是 West Gate Networks 公司的总裁。
原文信息	2019 年 12 月 31 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/networking/7-network-trends-you-can-expect-2020
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。