安天发布《Unique 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 Unique 的勒索软件变种，该勒索软件隶属于 IEncrypt 勒索软件家族，此变种于 2020 年 1 月被发现，主要通过垃圾邮件和 RDP 爆破进行传播。

Unique 勒索软件执行后，加密计算机上的文档文件，在原文件名后追加名为“.un1que”的后缀，每加密一个文件都会在该文件同一目录下创建名为“原文件名+.un1que_readme”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 USER_ID 等。Unique 勒索软件使用“RSA+AES”加密算法加密文件，将自身移动至系统临时目录下，并利用 Windows 系统 NTFS 文件流（ADS）技术实现隐藏，通过 ARP 和 NSLOOKUP 命令扫描局域网主机，对存活主机进行探测。调用命令行命令来防止受害者恢复文件，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、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、 字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器等鉴定分析。

最终依据动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	unique.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	156 KB
MD5	8116E91FEC95489C642BD30A402960BA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ransom
判定依据	动态行为

◆ 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
删除全盘所有卷影副本	★★★★
在启动时禁用 Windows 错误恢复	★★★★
查询系统硬盘大小	★★★
利用文件流隐藏	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取系统信息	★
获取计算机名	★
检索系统内存信息	★
WMIC 调用执行	★★
获取计算机用户名	★
获取驱动器类型	★
扫描磁盘类型	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★★
删除日志信息	★
释放 PE 文件	★
设置文件属性为隐藏	★

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 2 月 17 日 (总第 218 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天工程师编写可视化小工具助力安全复工

当前，新型冠状病毒肺炎疫情防控形势严峻，春节长假结束后还将迎来返程高峰，为有效防控疫情，多个省市作出了延迟企业复工复业的决定。对于企业机构，需要了解掌握当前员工的全国分布情况和所面临的疫情风险程度，做好员工相关的保障需求分析和返程安排。安天可视化研发中心的工程师紧急编写了这款名为 Antiy_SAT 的可视化小工具，以协助企业机构可视化分析员工分布和返程情况，做好防疫保障。

疫情牵动着安天人的心，安天的移动安全公司就处于疫情防控任务最为艰巨的武汉。为支持安天内部疫情响应保障需求，同时有效支撑起疫情期间的应急值守和响应工作，安天可视化研发中心的工程师们在节日期间借助安天数据分析平台编写了公司人员分布情况分析模块，后又根据安天部分产品客户提出的要求，将相关功能变成本地化模块提供给客户试用。现将这个小工具发布，给有需要的政企机构使用。

图一：显示人员在不同时点地域分布情况

图二：显示不同日期的人员返程情况

Antiy_SAT 是一款完全本地化的工具，用户按照手册要求，对应数据表格式，将本单位情况导入并转换为相关数据格式，即可直观的了解企业员工分布和返程情况，协助各单位指导和安排员工工作，为节后开工及疫情后续相关工作提供一定的参考和辅助。

说明

● 该工具软件支持版本升级和近期每天疫情更新。为保护用户数据安全，只在本地执行，不会上传用户数据。

● 安天工程师每天会更新一次工具包，包中疫情数据会更新为前一日公布的疫情数据。

● 本工具及相关资料由安天安全可视化研发中心开发和编撰，可以免费使用，不得用于商业用途，如需二次发布请保留安天的版权信息和 logo。

● 本工具中使用了开源代码和多种字体，工具文档中进行了明示，并表示感谢。

● 若在使用过程中有任何问题，欢迎在论坛留言讨论，我们会提供持续的支持。

此外，安天推出一系列力所能及的举措

当前，新型冠状病毒感染肺炎疫情防控工作已进入关键时期，为有效保证医疗卫生系统的健康运行，安天推出了一系列力所能及的举措。

专家团队 24 小时值守

从 1 月 27 日开始，安天客服热线已经由客服值守改为专家团队值守，为全国医疗卫生系统提供免费安全咨询和应急响应服务。

智甲医疗行业版免费服务新型肺炎定点医院

作为安天主打产品之一的安天智甲终端防御系统医疗行业版将面向全国收治新型肺炎的定点医院提供两年免费服务。可直接拨打安天 400-840-9234 电话获得相关产品使用指导。

发布三款安全工具免费版本

安天发布三款安全工具的免费版本，Atool 系统安全分析工具、Scan Tool 精细化扫描工具和 Action Scope 轻量级文件行为分析工具，以有效支撑疫情期间可能的应急响应与处置工作。

7*24 小时专线：400-840-9234

应急信箱 :cert@antiy.cn

安全技术专家团 值守响应！

让我们一起携手，共抗疫情！

可视化安全工具及三款安全工具
免费版本的下载地址见安天创意论坛

安全厂商发现 Windows 感染式病毒 KBOT

卡巴斯基最近发现了通过将恶意代码注入 Windows 可执行文件而传播的恶意软件，换句话说，就是病毒。卡巴斯基将其命名为 KBOT，卡巴斯基解决方案将恶意软件及其组件检测为 Virus.Win32.Kpot.a，Virus.Win64.Kpot.a，Virus.Win32.Kpot.b，Virus.Win64.Kpot.b 和 Trojan- PSW.Win32.Coins.nav。KBOT 病毒造成了严重的威胁，因为它能够通过感染可执行文件在系统和本地网络上迅速传播，而且不可能恢复。它通过向系统进程注入数据显著地降低了系统速度，使其处理程序能够通过远程桌面会话控制受损的系统，窃取个人数据，并执行 web 注入以窃取用户的银行数据。

（原文链接：https://securelist.com/kbot-sometimes-they-come-back/96157/）

每周安全事件

类 型	内 容
中文标题	安全厂商发现 Windows 感染式病毒 KBOT
英文标题	KBOT: sometimes they come back
作者及单位	Anna Malina
内容概述	卡巴斯基最近发现了通过将恶意代码注入 Windows 可执行文件而传播的恶意软件，换句话说，就是病毒。卡巴斯基将其命名为 KBOT，卡巴斯基解决方案将恶意软件及其组件检测为 Virus.Win32.Kpot.a，Virus.Win64.Kpot.a，Virus.Win32.Kpot.b，Virus.Win64.Kpot.b 和 Trojan- PSW.Win32.Coins.nav。KBOT 病毒造成了严重的威胁，因为它能够通过感染可执行文件在系统和本地网络上迅速传播，而且不可能恢复。它通过向系统进程注入数据显著地降低了系统速度，使其处理程序能够通过远程桌面会话控制受损的系统，窃取个人数据，并执行 web 注入以窃取用户的银行数据。
链接地址	https://securelist.com/kbot-sometimes-they-come-back/96157/

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.CubeSpy.a[prv,exp,spy] 2020-02-07	高	该应用程序运行后隐藏图标，会私自窃取用户安装的应用信息、通话记录、通讯录、地理位置、短信记录、固件信息、网络信息、通知栏消息、app 使用记录，并将其私自上传到服务器，还能下载未知 apk 自动安装，造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.InfoStealer.ar[prv,fra] 2020-02-08	中	该应用程序伪装为表白软件，运行后会上传用户电话号码，通讯录，通话记录和短信至服务器，造成用户隐私泄露，建议卸载。
		RiskWare/Android.Clicker.aj[exp] 2020-02-09	低	该应用程序伪装为 Android 版的 siri，运行无实际意义，点击展示图片，警惕其推送广告造成用户的资费消耗，建议不要使用。
	较为活跃样本	Trojan/Android.spymax.b[prv,rmt,spy]	中	该应用程序是一款间谍软件，运行后隐藏图标，联网私自下载恶意间谍子包，窃取用户地理位置、wifi 信息、私自拍照、录像。造成用户隐私泄露，建议卸载。
		Trojan/Android.PuaImei.a[prv,spy]	中	该应用程序伪装正常应用，包含风险代码，运行通过借助无障碍服务获取用户行为信息、短信信息等并上传，造成用户的隐私泄露和资费消耗，建议卸载。
		Trojan/Android.Joker2.o[prv,pay,exp]	中	该应用程序伪装正常应用，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息，造成用户隐私泄露和资费消耗，建议卸载。
		G-Ware/Android.SmsSend.py[exp,rog]	中	该应用程序运行隐藏图标，私自发送短信到指定号码，造成用户资费消耗，建议卸载。
		Trojan/Android.Dropper.dw[rog]	低	该应用程序私自下载、静默安装未知 apk，推送广告，造成用户流量资费损失，影响安全性，建议卸载该应用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Excel 远程代码执行漏洞（CVE-2020-0650）	高	当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发一个远程代码执行漏洞。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，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序；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.Yakes	中	此威胁是一种木马类程序。该家族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/Win32.Bublik	中	此威胁是一种以窃取用户敏感信息为目的的木马类程序。该家族样本运行后，会安装恶意浏览器工具栏和扩展工具，引起搜索结果重定向等问题。该家族通过电子邮件或捆绑安装等方式进行传播。
		Trojan[Clicker]/Win32.Agent	中	此威胁是一种具有点击行为的木马类程序。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，弹出广告窗口，使浏览器重定向至其他网页。该家族会为黑客打开后门，允许黑客窃取用户信息。
		RiskWare[Downloader]/Win32.AdLoad	中	此威胁是一种下载广告软件的风险软件类程序。该家族可以入侵用户系统；窃取重要数据，同时在被感染的电脑中安装恶意软件，使用户的电脑性能降低。
		RiskWare[Downloader]/Win32.Monstruos	中	此威胁是一种以下载为目的的风险软件类程序。该家族安装后，会在电脑中下载并执行其它恶意代码。该家族利用垃圾邮件等方式进行传播。

2020 年值得关注的五大安全趋势和预测

约翰·贝克尔 / 文 安天技术公益翻译组 / 译

纵观 2019 年的网空安全态势，我们发现攻击依旧频频发生。网络犯罪分子针对全球各地的组织机构和个人不断地发起各种攻击，从卷土重来的勒索软件攻击到大规模的数据泄露事件。2019 年除了攻击数量庞大之外，网络安全行业还观察到将新旧威胁相结合的攻击。黑客将其传统的攻击手段，如网络钓鱼、僵尸网络、恶意软件和 DDoS，与人工智能（AI）和机器学习（ML）结合起来，从而发起更加复杂的攻击。

但是 2019 年不光只有威胁在演变。正在开发以用于反击这些攻击的技术在不断发展，赋予给安全的企业“价值”也在不断提高。组织机构正在加大对安全研究团队和漏洞赏金计划的投资，新的培训资源也正在帮助公司减少内部威胁。

随着我们步入 2020 年和新的十年，有许多关于网空安全的预测和趋势成为头条新闻。以下是五个值得我们关注的趋势和预测：

合格的网络安全专业人员短缺加剧

随着 2020 年的到来，技能娴熟的网络安全专业人员短缺问题仍然是网络安全行业所面临的头等大事。根据（ISC）2 发布的《2019 年劳动力报告》，目前全球约有 130 万个网络安全职位空缺。仅仅在美国，CyberSeek（美国 NIST 支持的一项全美网络安全教育 (NICE) 计划。其主要功能是能在线查询全美、各州的网络安全人才供需差距。）目前显示的职位空缺就超过 50 万个，这些职位的平均底薪约为 9.6 万美元。为帮助改变这一趋势，网络安全行业必须继续采取多管齐下的方式。这不仅需要着眼于创造能够赋能专业人员的技术，同时还需要在正规教育和人才发展计划的基础上扩大人才储备。

你能够应对云安全问题吗？

人们对云的方方面面的担忧也在不断增加，包括云数据丢失、未经授权的访问、错误配置、加密等方面。实际上，有 93% 的组织机构都在适度甚至极度关注云安全。但是，在 2020 年组织机构将如何应对云安全所面临的这些挑战才是人们感兴趣的话题。围绕这一话题的预测也层出不穷，正如一些专家所预测的，错误配置的增加会导致更多的数据泄露，而另一些专家则希望通过新的 SaaS（软件即服务）SIEM（安全信息和事件管理）解决方案和联盟来推动市场的发展。

让人工智能和机器学习成为我们的工具

从网络安全攻防双方来看，打个比方，如果人是乌龟，那么威胁就是野兔。尽管我们可能无法跟上大量针对网络发起的攻击的步伐，但围绕人工智能和机器学习的创新正在帮助我们加快针对这些威胁（尤其是新威胁）的早期识别和响应。可不幸的是，黑客也在利用这些技术来获取关于人工智能模型的知识，以便将恶意代码更好地隐藏在应用程序中，等等。当我们步入 2020 年，我们会看到新的利用人工智能建模的恶意软件，它们能够逃避沙箱检测，或者使用人工智能驱动的鱼叉式网络钓鱼攻击，从而进一步扩大攻击的规模。

网络安全和风险管理成为首席信息官（CIO）的首要任务

美国国家首席信息官协会（NASCIO）表示，对于 2020 年的战略、政策和管理流程来说，网络安全是首要问题。安全性增强工具在他们的十大技术排名中位于第四，云解决方案、老旧应用程序现代化和数据分析分别排在前三位。有趣的是，弗雷斯特研究公司（Forrester Research）2020 年的预测主要集中在另一些不同的挑战上，其中包括人才招募和保留、数据策略和自动化。

物联网安全问题日益严重

对于负责保护公司网络安全的安全团队而言，物联网设备的兴起将继续给他们带来挑战。随着物联网攻击在 2019 年的大幅增加（卡巴斯基报告称，物联网攻击从 2018 年上半年的 1200 万次增至 2019 年上半年的 1.05 亿次），许多业内人士预测，黑客利用被入侵的设备发动大规模攻击，围绕这一攻击向量的攻击将大幅增长，这并不令人意外。要想对抗这种威胁，组织机构必须增加其监控的攻击面，利用可简化管理的新解决方案，并减少误报，因为这些误报常常会导致 IoT 的安全解决方案失效。《CISO 杂志》最近发表的一篇文章也概述了一些比较特殊的攻击，包括针对联网加油站和联网咖啡机的攻击。

我们会很容易发现十个到二十个更值得关注的趋势、预测和挑战。我们一定要密切关注 2020 年的网空安全态势。

原文名称	5 Security Trends and Predictions to Watch in 2020
作者简介	约翰·贝克尔（John Becker）。约翰·贝克尔是 Bricata 公司的总裁。
原文信息	2020 年 1 月 28 日发布于 Security Boulevard 原文地址 https://securityboulevard.com/2020/01/5-security-trends-and-predictions-to-watch-in-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。