安天发布《Makop 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Makop 的勒索软件，该勒索软件于 2020 年 2 月初被发现，其传播方式主要为垃圾邮件。Makop 勒索软件主要针对医疗卫生行业，在当前防治新型冠状病毒时期，对医疗卫生行业造成巨大网络安全威胁。

Makop 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“.[USER_ID].[联系邮箱].makop”的后缀，在计算机桌面上创建名为“readme-warning.txt”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 USER_ID 等。Makop 勒索软件运行后修改注册表项，以达到开机自启动的目的，同时在初次加密完成后，该勒索软件会监控文件系统，每隔 30 秒扫描新增的未加密文件，并对未加密文件进行加密。Makop 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、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、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	makop.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	31 KB
MD5	2EF9CA2508D649500348C8712229E97B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Crypt]/Win32.Ransom
判定依据	BD 静态分析

完整报告地址：https://1.119.163.6/vue/details?hash=2EF9CA2508D649500348C8712229E97B#kk_executer_win7other_behavior 1/143

◆ 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

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
Run 自启动	★
获取计算机名	★
检索系统内存信息	★
获取驱动器类型	★
创建挂起进程	★★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
访问文件尾部	★
文档篡改	★★
创建快捷方式	★
设置文件属性为隐藏	★★
感染文件	★★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.1	67	192.168.122.165	68
192.168.122.165	60434	224.0.0.252	5355
192.168.122.165	65417	224.0.0.252	5355
192.168.122.165	57202	224.0.0.252	5355
192.168.122.165	55609	224.0.0.252	5355
192.168.122.165	54286	224.0.0.252	5355
192.168.122.165	52972	224.0.0.252	5355
192.168.122.165	57625	224.0.0.252	5355
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 3 月 02 日 (总第 220 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天为远程办公提供安全接入和综合安全保障方案

在全民抗疫的大环境下，多数企业都采取了远程办公的工作模式。而在工作模式转变的过程中，远程办公业务场景下的整体安全防护工作也面临大量新的威胁挑战，其中最突出的问题在于：

1、远程办公环境下主机不可控、接入条件不可控、使用者不可控，如何保证系统和数据的安全？

2、大量远程办公设备接入内网以及差异化的业务系统访问需求，如何减小连带的安全风险和横向移动？

3、企业内网出现安全威胁，应急响应工程师无法抵达现场该如何进行远程应急响应处置？

在此背景下，安天集团迅速整合端点防护、安全监测、安全可视化等产品部门，以旗下安天移动安全智信零信任应用安全交付系统产品为主干，迅速完善远程办公安全整体解决方案。从构建便捷安全的接入与管控能力、保障安全可靠的接入环境、增强内网监测管控能力、建立安全响应第二通道等维度出发，以零信任架构为基础，为企业远程办公业务场景提供全过程、高安全、便捷可靠的综合安全解决方案，协助客户实现远程办公主机本地环境的安全加固与防护，构建零信任的虚拟安全边界、统一身份认证和动态的访问策略管控能力，增强内网安全监测管控与远程响应处置能力。

方案架构图

方案架构

安天远程办公综合解决方案以零信任架构为基础，协助客户重构虚拟安全边界，并提供更加安全的应用访问环境和内网安全监测与远程安全响应措施。方案由零信任应用安全交付、终端安全防护、内网安全监测、远程应急响应和定制可视化指挥舱等部分组成，为政企机构远程办公业务场景的接入使用、安全管理、安全监测、安全处置、安全决策提供全方位安全能力支撑。

- 为远程接入用户提供多维安全防护的终端环境，保障安全的远程办公环境；
- 为企业内网及业务系统提供统一身份、多因子认证、单点登录和链路透明加解密等措施，保障应用访问入口安全；
- 为企业安全管理者提供基于身份、状态、行为、内容的零信任策略手段，构建应用访问控制策略的动态管控能力；
- 为企业安全管理者提供深度威胁检测和分析措施，增强内网安全监测管控与高级威胁发现能力；
- 为企业安全处置人员提供远程应急响应、威胁检测、分析、处置、取证等配套工具，构建远程应急处置通道；
- 为企业管理者提供员工行为画像、信誉评估等整体安全态势，按需打造可视化指挥舱支撑企业安全决策。

特点优势

● 20 年威胁检测与防护能力

安天拥有自主领先的威胁监测分析能力，在 PC 场景和移动场景威胁检测与防护能力有长期积累，在主机安全检查与加固、主动防御和 Wi-Fi 安全、短信安全、扫码安全、数据隐私安全等方面能力基础深厚。

●多场景动态策略管控

基于零信任安全架构，提供基于用户身份、行为、内容、环境的动态安全访问控制策略，内置多种安全策略模型，可基于场景需要灵活配置和选择。

●多端协同保障数据安全

覆盖“访问、交互、传输、存储”立体化数据安全防护，基于国密算法的链路加密，拥有终端防截屏、防复制粘贴、基于身份的透明水印、文档不落地浏览等功能；以及终端手机数据加密，关键数据使用白盒密钥加密，服务端数据存储加密等功能。

●高效率远程响应处置

通过远程协助工具建立起处置现场与远程专家团队的技术通道，高效实现技术能力的最大输出。

●灵活交付快捷上线

灵活的交付模式适合不同的部署场景，不影响现有网络结构，支持多种认证方式，无改造单点登录，一键生成移动端应用，PC 环境良好适配低占用。

客户支持

全国服务热线：400-840-9234

售后支持邮箱：support@antiy.cn

以上内容为精简版
微信扫描二维码即可阅读全文

每周安全事件

类 型	内 容
中文标题	恶意软件伪装成新型冠状病毒查询程序感染用户
英文标题	South Korea suffers from the spread of people infected with Corona 19
作者及单位	Pierluigi Paganini
内容概述	发现的恶意软件是一个可执行程序 (EXE)，使用“冠状病毒 (corona) 的国内状态”和“冠状病毒的实时状态”等文件名。运行该文件时，用户将看到一个名为“实时 Corona19”的弹出窗口。恶意程序会将实际载荷释放到受感染主机的临时文件夹下，用户主机一旦被该恶意代码感染，受害主机将面临被远程控制、屏幕截图、安装其它恶意软件和信息劫持。
链接地址	https://securityaffairs.co/wordpress/98420/malware/south-korea-corona-19.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.bigbustown.c[prv,exp] 2020-02-23	高	该应用程序伪装其他应用，运行隐藏图标，激活设备管理器，监听用户的短信、通知栏信息，后台联网下载银行木马相关子包，利用银行相关钓鱼界面窃取用户银行相关信息，会造成用户隐私泄露和资费消耗，建议卸载。
		Trojan/Android.batMonitor.a[prv,rmt,rog] 2020-02-24	中	该应用程序伪装 Google System Service，运行后台会置顶设置页面，拦截短信，获取用户短信、联系人、手机安装包等信息，调用设备摄像头拍照等，连接服务器执行远程命令，并发送短信到指定手机号码，造成用户隐私泄露及影响用户使用，建议卸载。
		G-Ware/Android.FakeSystem.bi[rog,exp] 2020-02-25	低	该应用程序伪装系统应用，运行隐藏图标，后台访问广告信息并展示，会造成用户流量资费损耗，请卸载。
	较为活跃样本	Trojan/Android.LockScreen.cx[rog,lck]	中	该应用程序包含恶意代码，运行后激活设备管理器，锁定屏幕勒索用户加 qq 解锁，影响用户手机的正常应用，建议卸载。
		Trojan/Android.FakeFB.ae[prv]	中	该应用程序伪装成 Facebook，运行通过发送短信的方式窃取用户输入的账号密码，造成用户隐私泄露和资费消耗，建议卸载。
		Trojan/Android.B4ABanker.b[prv,exp]	中	该应用程序伪装金融相关软件，运行后隐藏图标，诱导用户填写银行相关隐私信息，并通过网络上传，造成用户隐私泄露，建议立即卸载。
		Trojan/Android.Banbra.e[prv,exp]	中	该应用程序包含恶意代码，运行后台联网可能下载银行木马子包文件，并反射调用，警惕造成用户资费消耗和隐私泄露，建议卸载。
		RiskWare/Android.Fakejiaoyou.k[fra,exp]	中	该应用程序伪装交友软件，通过发送虚假诱惑性消息，诱导用户付费充值 vip，及填写用户详细信息，造成用户信息泄露和经济损失，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows LNK 远程执行代码漏洞 (CVE-2020-0729)	高	Microsoft Windows 在处理 .LNK 文件过程中存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。攻击者可能会向用户发送包含恶意 .LNK 文件和关联的恶意二进制文件的可移动驱动器或远程共享。当用户在 Windows 资源管理器中打开此驱动器（或远程共享），或打开可解析 .LNK 文件的其他任何应用程序时，攻击者即可在目标系统上执行代码。
	较为活跃样本	Trojan/Win32.SGeneric{S:DS}	中	此威胁是一种木马类程序，是使用启发式方法检出的家族。该家族运行后会同时释放出恶意程序和正常程序，用正常程序来掩盖恶意程序；该家族还会引起杀毒软件和个人防火墙无法打开，甚至在杀毒软件运行时使电脑会出现蓝屏、自动重启、死机等状况。
		Trojan[Banker]/Win32.Banz	中	此威胁是一种窃取网银信息的木马类程序。该家族样本运行后会利用系统漏洞感染用户电脑，以获取用户的银行密码、信用卡号码等敏感信息。该家族会修改注册表，降低系统性能，破坏系统文件。
		Trojan[Dropper]/Win32.Binder	中	此威胁是一种具有捆绑行为的木马类程序。该家族运行时会携带各种恶意软件，并在电脑中进行安装。该家族还会窃取用户信息，占用系统资源，影响用户使用电脑。
		GrayWare[AdWare]/Win32.MultiPlug	低	此威胁是一种广告类灰色软件程序。该家族具有反虚拟机、反调试功能，运行后会添加自启动项，并弹出广告，具有一定风险。
		GrayWare[AdWare]/Win32.Amonetize	低	此威胁是一种以安装广告为目的的灰色软件类程序。安装该家族的样本时可选择自定义安装。在安装过程中，捆绑的广告软件被安装至用户电脑，这可能威胁用户的操作系统。

七种可防止网空攻击的关键防火墙功能

鲁斯·舍费尔 / 文 安天技术公益翻译组 / 译

为什么最先进的智能防火墙对您的业务的安全性和成功来说至关重要？

防火墙技术曾经很简单易懂。您使用组织机构设置的预定义安全策略对其进行编程。然后，防火墙会对传入和传出的流量进行过滤，让安全的流量进入您的网络，同时将危险的流量排除在外。但在防火墙问世之后的四十年里，安全技术和网空犯罪方法都有所发展。

随着企业采用云计算、软件即服务（SaaS）应用、移动和物联网（IoT）设备，企业 IT 在 2020 年将继续变得更加互联，更容易受到网空攻击。将物联网设备连接到您的网络，为黑客攻击提供了更多的入口点。这些安全问题几乎会影响每家公司，67%的公司已经经历过物联网安全事件。您的公司会成为下一个网络攻击受害者吗？

合规性、隐私和数据安全不再只是 CISO 和 CIO 关心的内容，它们对 CEO 和公司董事会来说也很重要。鉴于所有企业面临的网空攻击风险都在不断增加，企业有必要使用智能和创新的下一代防火墙（NGFW）来保护其网络，该防火墙应包括以下七个关键功能：

功能 1：管理

下一代防火墙（NGFW）最需要的就是统一的安全管理平台。NGFW 需要出色的安全管理和高效的特性，以满足现代分布式企业对云、数据中心、移动设备、PC 和物联网的需求。安全管理不仅仅是安全策略以及网络和设备配置。您还必须考虑易用性、提高运营效率和统一的平台。其他关键特性还包括能够扩展安全性的能力，以匹配 IT 网络的增长、自动化工作流以及在整个安全基础架构中维持一致的策略实施。

功能 2：威胁防护

包括反网络钓鱼、反病毒和反僵尸网络在内的核心威胁防护技术超越了传统的防火墙安全功能，后者仅与 IPS 简单集成以整合硬件。基于云的分析和威胁情报提供了进一步的威胁防护优势，包括自动更新恶意特征码。

功能 3：应用程序检查和控制

随着企业的发展和规模扩大，企业有必要选择具有足够广泛的应用程序支持的防火墙，以识别新的、复杂的应用程序。随着时间的推移，防火墙正朝以下几个方向发展演化：广泛、深入、智能和动态。

功能 4：动态、基于身份的检查和控制

由于转向动态寻址、云架构和基于组的策略，基于简单 IP 地址的传统防火墙规则正在发生变化。企业需要一个防火墙，它可以支持基于第三方用户存储、公共和私有云对象、外部服务源（如 Office 365、AWS 地理位置）以及新设备类（如物联网）的策略。使用威胁情报和自动化来实现动态策略创建和实施也很重要。智能自动化将减少手动配置更改和容易发生的人为错误，从而降低安全风险和成本。

功能 5：混合云支持

为了满足以云优先企业的需求，您的下一代防火墙应该通过提供基于动态工作负载的可扩展性能，以及用于经济高效部署的消费模型，来实现云的自动化和编排。

功能 6：安全和性能同步提升

随着需求的增加，您的下一代防火墙将需要确保功能的可扩展性。下一代防火墙没有了能够阻止企业部署最新威胁检测技术和算法的硬件限制，这一点非常重要。因为传统的防火墙的性能表现往往就受硬件性能的制约。NGFW 部署在云中，如果云中的硬件资源使用也受限，则同样会极大影响其性能表现。超大规模网络安全技术可在本地实现云级安全，并可根据吞吐量和安全性需求的变化来扩展性能。

功能 7：加密流量检查

谷歌最近的一项调查表明，终端用户的 Chrome 浏览器活动所产生的网络流量中，有 90%以上是经过加密的。随着加密流量的增加，网空威胁变得更加高级和更具破坏性，您的防火墙需要对这些流量进行检查，以便应用控制策略并激活威胁防护。

整体分析

许多组织机构必须使用多种安全解决方案来支持复杂的安全体系架构，这样可能会导致集成复杂、配置错误以及运营效率低下。在选择下一代防火墙或企业防火墙时，全面考虑安全架构和安全运营非常重要。如您所见，下一代防火墙不仅仅是网络流量策略的实施要点。这些防火墙实际上是智能安全网关，其中包括应用程序智能和多维威胁防护。

原文名称	7 Critical Firewall Capabilities to Prevent Cyberattacks
作者简介	鲁斯·舍费尔（Russ Schafer）。鲁斯·舍费尔是 Check Point 公司安全平台的产品营销主管。
原文信息	2020 年 2 月 10 日发布于 Dark Reading 原文地址 https://www.darkreading.com/7-critical-firewall-capabilities-to-prevent-cyberattacks/d/d-id/1336980
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。