安天智甲有效防护 WANNACASH NCOV 勒索软件变种

近日，安天 CERT 在梳理网络安全事件时发现一个名为 WANNACASH NCOV 的勒索软件变种，该勒索软件隶属于 WannaCash 勒索软件家族，最早于 2020 年 3 月被发现，主要通过垃圾邮件进行传播。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 WANNACASH NCOV 勒索软件的加密行为。

WANNACASH NCOV 勒索软件执行后，加密计算机上的重要文件，将原文件名修改为“Файл зашифрован. Пиши. Почта clubnika@elude.in [数字].WANNACASH NCOV v310320”，文件名中俄语部分译为文件已加密请发邮件，修改桌面背景为勒索提醒并在计算机桌面上创建名为“Как расшифровать файлы.txt”（译为如何解密文件 .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、联系方式等。WANNACASH NCOV 勒索软件执行后会弹出一个名为“keys.txt”的文件，操作注册表在启动项创建新的键值。WANNACASH NCOV 勒索软件使用“AES+RSA”加密算法加密文件，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、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、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、反病毒引擎鉴定器、关联分析鉴定器、信标检测鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	b4a77a2ee0c31c3ef24ef09ecd0b238140f97ad16afaafa73b146399e77a983a
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.13 MB
MD5	F991B2C2850E32AA1D55B9EAC221FBF3
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Encoder
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
创建可疑进程	★★★★
伪装打开 TXT 文本	★★★★
堆喷射	★★★★★
访问下载站点	★★★
删除自身	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
检测自身是否被调试	★★
Run 自启动	★
获取驱动器类型	★
获取计算机名	★
检索系统内存信息	★
获取当前激活的窗口	★★
.....	.....

◆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 4 月 27 日 (总第 228 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

率先完成全平台兼容适配 安天智甲成为统信操作系统生态伙伴

4 月 21 日，安天旗下的智甲终端防御系统（以下简称：安天智甲）完成与统信操作系统 UOS 的四项测试内容，安天是率先完成与统信操作系统 UOS 全平台适配兼容的安全厂商。

统信软件推出的统一操作系统 UOS 是我国自主创新的新一代操作系统。此次认证安天智甲分别通过了“鲲鹏、飞腾、龙芯、海光、兆芯、X86、申威”七个平台的“统信服务器操作系统和统信桌面操作系统”产品兼容性测试、产品功能性测试、产品性能测试和产品安全可靠性测试，满足兼容认证要求，成为统信软件产品生态伙伴。

安天是国内较早研发国产操作系统终端防护产品的安全厂商，亦有 20 年端点安全技术积累与实战经验。安天智甲终端防御系统是聚焦企业、政府、军队等业务网络研发的终端安全防护产品。安天智甲完全自主研发，具有自主可控的反病毒引擎，可对各种蠕虫、木马、宏病毒等恶意代码进行检测和清除，通过行为分析对未知威胁进行拦截。满足等级保护、分级保护要求，同时也可对信创领域的通用国产计算机和涉密国产专用机进行全方位安全防控。

未来安天将坚持自主创新脚步，领先布局国产化安全领域，积极响应国家政策和要求，推进国家安全自主创新蓬勃发展。

微信扫描二维码阅读原文

CNCERT 发布《2019 年我国互联网网络安全态势综述》报告

2020 年 4 月 20 日，国家互联网应急中心（CNCERT）编写的《2019 年我国互联网网络安全态势综述》报告（以下简称“2019 年态势报告”）正式发布。为全面反映当前我国网络安全的整体态势，CNCERT 自 2010 年以来，每年及时发布前一年度网络安全态势情况综述，至今已连续发布 11 年，对我国党政机关、行业企业及全社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。

（原文链接：https://mp.weixin.qq.com/s/uQPWQGrGMUg60FOoMVesNw）

钓鱼邮件冒充 Zoom 和 WebEx 窃取用户凭证

Proofpoint 研究人员发现并记录了针对不同行业的美国公司的电子邮件钓鱼活动，其中包括模仿 Zoom 和 Cisco（WebEx）的电子邮件。攻击者不仅利用视频会议品牌作为恶意软件的诱饵，还利用它进行窃取凭证，特别是盗取 Zoom 和 WebEx 的凭证。被盗的账户凭证可能被用来登录公司视频会议账户，也可能在黑市上出售，或用于获取更多关于攻击目标的信息。

（原文链接：https://www.helpnetsecurity.com/2020/04/21/phishing-zoom-webex/）

研究人员发现影子经纪人泄露事件的新 APT 组织

2017 年 4 月 14 日，一群被称为“影子经纪人”(Shadow Brokers) 的神秘黑客发布了一系列黑客工具，最终彻底改变了互联网。泄漏中最知名的文件是永恒之蓝 (ETERNALBLUE)，其中有一个名为 "sigs.py" 的文件，它包含 44 个签名，用于检测其他黑客组织部署的文件（黑客工具），编号从 1 到 45，缺少 # 42。但是，今年，在 OPCDE 虚拟网络安全峰会上的一次演讲中，一位安全研究人员发现了一种新的 APT- 位于签名 # 37 后面，研究人员纠正了将 37 号签名错误地归因于疑似与中国有关的网络间谍组织 Iron Tiger。研究人员表示，他认为这个组织可能位于伊朗，据在恶意软件中找到的字符串将其命名为 Nazar APT。

（原文链接：https://www.zdnet.com/article/security-researcher-identifies-new-apt-group-mentioned-in-2017-shadow-brokers-leak/）

微软发布针对 Autodesk FBX 库的带外安全更新

微软发布了一项带外安全更新，修复了集成到微软Office和Paint 3D应用中Autodesk FBX库中的远程代码执行漏洞。成功利用这些漏洞的攻击者可以获得与本地用户相同的用户权限。要利用这些漏洞，攻击者必须将包含3D内容的特制文件发送给用户，并说服用户打开它。该安全更新通过更正Microsoft软件处理3D内容的方式来解决这些漏洞。

（原文链接：https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-oob-security-updates-for-microsoft-office/）

每周安全事件

类 型	内 容
中文标题	攻击者利用 Agent Tesla 间谍软件针对能源公司
英文标题	Oil and Gas Firms Targeted With Agent Tesla Spyware
作者及单位	Lindsey O'Donnell
内容概述	攻击者正在利用 Agent Tesla 间谍软件以能源公司为目标，正如最近带有恶意附件的鱼叉式钓鱼邮件所显示的那样。这些电子邮件充分利用了当今石油和天然气市场动荡的性质，攻击者利用人们对这次危机的担忧，冒充埃及著名的工程承包商 (石油和加工工业工程公司，简称 Enppi)。研究人员说，被列为目标的能源公司分布在马来西亚、美国、伊朗、南非、阿曼和土耳其以及菲律宾等地。受害者多为石油和天然气、木炭加工、水力发电厂、原材料制造和大型商品运输行业。
链接地址	https://threatpost.com/oil-and-gas-agent-tesla-spyware/154973/

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.dtghUpload.g[exp,rog] 2020-04-20	高	该应用程序包含恶意代码，运行配合其他程序使用，执行 cmd 命令遍历获取系统安装包，后台发送短信，并有安装或卸载其它程序的能力，可能造成用户手机使用风险，请谨慎使用。
		Trojan/Android.Homeproxy.b[exp] 2020-04-21	中	该应用程序运行把用户手机变为代理，重定向访问其他网址，导致用户资费消耗，警惕其造成用户的隐私泄露，建议卸载。
		G-Ware/Android.kdssa.a[rog] 2020-04-22	低	该应用程序被恶意篡改植入恶意代码，会劫持广告模块进行刷量作弊，造成用户资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.Knobot.b[prv,rog]	中	该应用程序伪装为正常应用，开机自启，运行后隐藏图标并加载恶意子包，窃取用户短信、彩信信息，当用户尝试进入设置页面卸载时，会强制跳转界面，达到防卸载的目的，造成用户隐私泄露，影响手机正常体验，建议立即卸载。
		Trojan/Android.CellSpy.e[prv,spy]	中	该应用程序是一款间谍工具，程序运行会隐藏图标，获取固件信息、GPS 位置信息用户等隐私信息上传到指定服务器，造成用户隐私泄露，建议卸载。
		Trojan/Android.Locker.ca[rog,lck]	中	该应用程序为勒索软件，运行请求激活设备管理器，置顶界面勒索用户付费解锁，造成用户手机无法正常使用，建议卸载。
		G-Ware/Android.FakeSystem.bk[prv,exp,rog]	中	该应用程序伪装为系统应用，运行后隐藏图标，后台会推广加载广告，监听用户短信信息，有发送短信、彩信等功能，为避免造成用户隐私泄露及资费损耗，建议卸载。
		G-Ware/Android.Triada.bu[exp,rog]	低	该应用程序包含恶意代码模块，程序运行会后台联网获取广告子包，私自推送广告。造成用户流量消耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 安全漏洞（CVE-2020-0961）	高	当 Windows Office 访问连接引擎不能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目标系统上执行任意代码。攻击者可以通过诱使目标打开经特殊设计的文件来利用此漏洞。
	较为活跃样本	Trojan[Backdoor]/Win32.Simda	中	此威胁是一种带有后门功能的木马类程序，黑客通过后门操纵用户计算机。该家族可以通过垃圾邮件及恶意网站等方式进行传播。该家族的变种有多种功能，如后门、密码盗取器、木马下载器和感染文件等。像这样拥有多种功能变种的木马类程序较为罕见。
		Trojan[Spy]/Win32.SpyEyes	中	此威胁是一种间谍类木马程序。该家族可以在被感染的用户电脑中隐藏自身，同时阻止其他软件检测其注册表、文件等。该家族会将其恶意文件进行压缩，压缩后的文件只能通过指定密码才能打开，而密码隐藏在汇编堆栈中，因此压缩后的文件无法被访问。
		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。
		Trojan[Downloader]/Win32.Zeagle	低	此威胁是一种下载类木马程序。该家族样本运行后，添加注册表启动项达到随机启动的目的；与远程服务器连接，下载其它的恶意程序到本地运行。
		GrayWare[AdWare]/Win32.ArcadeWeb	低	此威胁是一种广告类的灰色软件程序。该家族是通过行为来定性的灰色软件家族。该家族的不同变种之间，很可能除了推送 ArcadeWeb 网站的广告之外没有任何的关联。ArcadeWeb 软件是服务于 ArcadeWeb 网站的广告软件，它不仅进行广告推送，还会收集系统中的用户信息。ArcadeWeb 网站提供多种免费的网页游戏以吸引用户。

从流行病学中吸取的四个关于网络安全的教训

迈克·劳埃德 / 文 安天技术公益翻译组 / 译

一位有流行病学知识背景的首席技术官介绍了计算机病毒传播与现实世界冠状病毒传播之间的相似之处。

几年前，我离开流行病学领域，成为了一名网络安全工作者，但现在的新冠疫情让我意识到了这两个领域之间的相似之处。我们可以从现实世界的病毒传播中吸取很多教训，并将其应用到维护网络世界的安全之中。

虽然并不明显，但信息在计算机网络上的传播和疾病传播的过程确实很像。它从最基本的层面开始——当您连接到互联网时，您就开启了流行病学家所谓的“近邻传播”过程，而网络专家则将其称为路由协议。一台路由器中的信息在路由器之间共享，会传递给其相邻路由器，然后以此方式继续传递下去，就这样您的信息如同疾病的传播一般，在网络中扩散开来。

最初的一些主要的计算机威胁被称之为“病毒”也并非巧合，它们的传播方式与生物病毒的传播方式类似，并具有与之相似的感染和繁殖策略。如果你曾经从同事那里收到过受感染的电子邮件，你就见证了这一策略的发展：攻击者发现，比起用陌生的电子邮件地址联系你，用你熟悉的电子邮件地址能更有效地传播病毒。

那么，对流行病的研究能给我们带来哪些可以应用到网络安全的知识呢？我认为有以下几点：

理解横向移动

就像疾病会在我们与别人有接触时进行传播。这就是为什么在我写这篇文章的时候，许多人被要求待在家里或是固定地方，以降低病毒在人群中横向传播的能力。很明显，人类网络是全球性的、相互关联的。这种疾病虽然始于一个国家，但却可以横向传播到偏远的小岛。

在网络世界中，攻击者发现最容易的方法是先突破低价值目标，然后再向外扩散以攻击更好的目标。这是为什么呢？我们无法保护所有网络中的每个端点。因此，攻击者首先找到一个被攻破的位置。虽然网络很大，但从一个地方到另一个地方不需要很多次横向移动。就如同航空旅行可以让我们从一个地方很快到达另一个地方，进而加速现实世界中的病毒传播。在线上社交网络中，横向移动是攻击者武器库中最好的工具之一。

在与冠状病毒的斗争中，我们待在家里以阻止它的横向传播。同样，数字防御者也需要打破网络病毒横向移动的模式，将数据隔离到不同的区域。这样可以防止感染转移到新的区域。

知道感染的位置

在与疾病的斗争中，愈加明显的一点是，一个国家抗疫效果的好坏差异取决于该国对疾病的检测数量。检测可以发现染病人员，进而进行防控或治疗。数字安全也是如此。我们很难知道哪个网络节点受到感染，而响应团队通常都在忙于应对已经开始传播的病毒。

对于现实世界中的疾病，我们使用接触者追踪的方法。如果刚刚得知一个人是携带者，你需要立即追踪他的接触者，对他们进行检测，并在必要时进行隔离。数字世界的接触者追踪面临的挑战要困难得多，因为计算机通过网络在许多不同和不断变化的方向上进行通信，这相当于在现实世界中你要追踪的人每天从一个国家飞到另一个国家。

在一场网络危机中，对于“这种感染是如何传播到这里的，接下来又会如何传播？”这个问题，很难给出答案。为了找到答案，安全团队需要在攻击发生前很好地规划网络，并了解组织机构的所有访问路径和正常的信息流。这并不容易，但如果我们在自动化和算法方面做得越来越好，就可以更好地分析这类挑战人类思维的问题。

放慢速度

为阻止疾病蔓延，全世界的人们待在家里，遵守“压平曲线”倡议，这一伟大的举措可以减轻已经不堪重负的医疗系统的压力。同样，减缓网络攻击的速度也会带来巨大的好处。我们知道无法阻止下定决心的攻击者或国家级行为体，但放慢他们的速度可以为你的传感器检测数字入侵者争取时间，这样你就可以对他们进行拦截或隔离。传统的保险箱也可以体现出这一点，其安全等级取决于可以抵抗非正常进入的时间长短。

基本安全至关重要

关于目前的 COVID-19 爆发，最重要且一直重复的建议始终是：洗手。这是我们第一道也是最好的防线。这在网络世界也一样：基本安全很重要。在数字领域，网络安全包括了解网络上的内容、设备的安全配置、网络的设置是否符合预期以及任何更改是否会影响安全性，这些都不容易大规模地持续进行——即使是简单的事情。现实世界的网络充斥着无意的安全问题；即使做到基本安全标准的 90% 也不够。对于安全团队来说，更重要的是，要在任何地方、任何时间都能很好地执行基本的控制。所以，请大家一定要确保基本安全！

原文名称	4 Cybersecurity Lessons from the Pandemic
作者简介	迈克 · 劳埃德（Mike Lloyd）。迈克 · 劳埃德是网络安全公司 RedSeal 的首席技术官。
原文信息	2020 年 4 月 16 日发布于 Dark Reading 原文地址 https://www.darkreading.com/operations/4-cybersecurity-lessons-from-the-pandemic/a/d-id/1337535
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。