安天发布《PXJ 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 PXJ 的勒索软件，PXJ 勒索软件最早于 2020 年初被发现，主要通过钓鱼邮件进行传播。

PXJ 勒索软件执行后，加密计算机上的图片、数据库、视频、文档和其他文件，在原文件名后追加名为“.pxj”的后缀，在计算机桌面上创建名为“LOOK.txt”的勒索信，勒索信内容包含勒索说明和联系邮箱，赎金金额尚未确定，但勒索信中表示赎金金额将在头三天后每天增加一倍，解密密钥将在一周之后销毁。PXJ 勒索软件运行后在勒索软件同一目录下创建名为“Res.AAABANIx93RdufO4”的文件。PXJ 勒索软件使用“AES+RSA”加密算法加密文件，运行后清空回收站，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。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	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	112 KB
MD5	5DC438C8C9AB91CCADBA1DE82AB481D9
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
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
查询系统硬盘大小	★★★
删除全盘所有卷影副本	★★★★
在启动时禁用 Windows 错误恢复	★★★★
感染文件	★★★★

◆常见行为

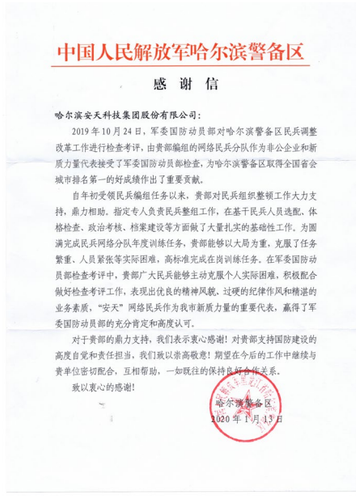
行为描述	危险等级
加载运行时 DLL	★
创建窗口	★
获取计算机名	★
获取驱动器类型	★
获取驱动加载权限	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
隐藏文件	★
扫描磁盘类型	★★
创建挂起进程	★★
.....	.....

◆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 3 月 30 日 (总第 224 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天收到哈尔滨警备区感谢信

近日，中国人民解放军哈尔滨警备区（以下简称：哈尔滨警备区）向安天发来感谢信，感谢 2019 年安天民兵网络分队作为非公企业和新质力量代表接受军委国防动员部检查，为哈尔滨警备区取得全国省会城市排名第一名的好成绩作出的重要贡献，并将安天民兵网络分队表彰为“优秀基层民兵先进集体”。


中国人民解放军哈尔滨警备区
感 谢 信
哈尔滨安天科技集团股份有限公司：
2019 年 10 月 24 日，军委国防动员部对哈尔滨警备区民兵调整改革工作进行检查考评，由贵部编组的网络民兵分队作为非公企业和新质力量代表接受了军委国防动员部检查，为哈尔滨警备区取得全国省会城市排名第一的好成绩作出了重要贡献。
自年初受领民兵编组任务以来，贵部对民兵组织整顿工作大力支持，鼎力相助。指定专人负责民兵整组工作，在基干民兵人员选配、体格检查、政治考核、档案建设等方面做了大量扎实的基础性工作。为圆满完成民兵网络分队年度训练任务，贵部能够以大局为重，克服了任务繁重、人员紧张等实际困难，高标准完成在岗训练任务。在军委国防动员部检查考评中，贵部广大民兵能够主动克服个人实际困难，积极配合做好检查考评工作，表现出优良的精神风貌、过硬的纪律作风和精湛的业务素质，“安天”网络民兵作为我市新质力量的重要代表，赢得了军委国防动员部的充分肯定和高度认可。
对于贵部的鼎力支持，我们表示衷心感谢！对贵部支持国防建设的高度自觉和责任担当，我们致以崇高敬意！期望在今后的工作中继续与贵单位密切配合，互相帮助，一如既往的保持良好合作关系。
致以衷心的感谢！
哈尔滨警备区
2020 年 1 月 13 日


松北区安天民兵网络分队：
在二〇一九年度工作中，被评为
优秀基层民兵先进集体
中国人民解放军黑龙江省哈尔滨警备区
二〇二〇年一月

此封感谢信，是哈尔滨警备区对安天民兵网络分队工作的肯定。作为网络大国向网络强国阔步迈进中的保卫者、引领威胁检测与防御能力发展的网络安全国家队，安天将执着探索、不断创新，牢记新使命，迈入新征程，捍卫祖国网络空间安全。

信息战争时代全民皆兵。2018 年 4 月，哈尔滨市民兵网络特殊分队在安天集团总部正式成立，接受地方人民武装部领导。自成立以来，安天网络民兵始终坚持把国家安全作为唯一立场和第一视角，始终坚定正确的政治方向，把筑牢思想“防火墙”做为重点，整合守护网络边疆与国家政治、军事、科技等安全开展职能教育，定期参加由上级部门指导的基干民兵综合素质训练，叫响“平时常用、急时先用、战时管用”口号，强化安天民兵“平时即战时，岗位即战位”的特殊属性。以主席嘱托鼓舞，以红色基因浸润，以军人作风强化，在八一、国庆等重大节日和参加五四精神寻访、徒步行、收看国庆 70 年阅兵直播等集体活动，坚持打军旗、穿军装、唱军歌、展军姿，增强军人荣誉感和身份认同感，圆满完成了全国“两会”、博鳌亚洲论坛、上合组织青岛峰会、中非合作论坛、世界军人运动会等重大活动安保任务。

疫情就是命令，防控就是责任。安天民兵网络特殊分队为满足企业机构了解掌握员工在全国动态分布情况和复工复产面临的疫情风险程度，方便企业预先做好员工的返程安排和复工保障，公司技术工程师、网络特殊分队队员，利用春节假期编写了“机构人员分布和返程分析”可视化工具，免费向社会开放。该可视化工具以全国疫情数据为基础，大数据分析隔离期员工数、异地员工数、员工健康状况、异常员工数、返程员工数等，综合梳理筛选在疫情期间员工的健康数据和节后返岗情况，配套做好防疫保障工作，助力企业安全复工复产。同时，为支持疫情响应保障需求，安天将一些相关功能变成本地化模块提供给政企使用，当月下载量达到 3900 余次。

安天网络民兵主动对接国防建设需求，为国防建设提供网络技术支撑和服务，全力建设军民融合的网络安全保障能力。立足于关键信息基础设施面临外方网络入侵渗透破坏的场景设定；以应急响应与分析处置工程师团队为骨干力量；通过安天“赛博超脑”平台提供的数据、样本分析能力、威胁情报输出及分析专家团队为后端支撑；以自主研发的应急处置工具箱、便携版流量监测系统、便携版沙箱分析系统等为携行装备。在应急处置、证据固化、风险排查、安全分析、追踪溯源方面完善基础科目能力，探索面向高级网空威胁猎杀的运行方法。

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	WildPressure 活动针对中东工业相关实体
英文标题	WildPressure targets industrial-related entities in the Middle East
作者及单位	Denis Legezo
内容概述	卡巴斯基研究人员在 2019 年 8 月发现了一个恶意活动，该活动分发了一个成熟的 C++ 木马，研究人员将其称为 Milum。该活动的受害者均为中东组织，包含与工业相关的部门。研究人员仅发现三个独特样本，因此认为该活动是具有针对性的，并将该活动命名为 WildPressure。样本文件编译时间戳均为 2019 年 3 月，攻击者使用租用的 OVH 和 Netzbetrieb 虚拟专用服务器（VPS）以及通过代理匿名化服务在 Domains 中注册的域。Milum 使用 JSON 格式存储配置数据，并使用 HTTP 作为 C2 通信协议。在 HTTP POST 请求中的加密通信中，研究人员发现恶意软件版本 1.0.1 的字段，这表示该恶意软件为开发的早期阶段。
链接地址	https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/

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.clevguard.b[prv,spy] 2020-03-22	高	该应用程序伪装为系统升级服务，运行后隐藏图标，激活设备管理器，窃取用户短信、联系人、通话记录、地理位置、手机固件信息、手机视频图片文件、wifi 信息、记事本信息、社交软件信息，私自通话录音、截屏，并将用户隐私上传至服务器。造成用户隐私泄露，建议卸载。
		Trojan/Android.PuaImei.b[prv,spy] 2020-03-23	中	该应用程序伪装为正常应用，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、浏览器输入等并上传，造成用户的隐私泄露和资费消耗，建议卸载。
		Trojan/Android.FakeJioPrime.c[exp,spr] 2020-03-24	低	该应用程序伪装为正常程序，无实际功能，运行私自群发推广链接短信，访问推广网页诱导用户下载安装，会造成用户资费损耗，请卸载。
	较为活跃样本	RiskWare/Android.Heineken.a[prv]	中	该应用程序运行后请求激活设备管理器，包含风险代码，触发下载未知应用，获取用户的联系人信息、邮箱等信息，联网上传用户 imei、sim 卡等信息，可能与其他应用配合使用，警惕其造成用户的隐私泄露，建议谨慎使用。
		Trojan/Android.CovidLock.a[rog,lck]	中	该应用程序伪装为新冠肺炎相关程序，运行诱导用户激活设备管理器，隐藏图标，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。
		Trojan/Android.SpyLoan.a[prv,rmt,spy]	中	该应用程序包含恶意代码，接收远程指令，上传用户短信、联系人、通话记录等隐私信息，造成用户隐私泄露，建议卸载。
		Trojan/Android.Knobot.a[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.SmsSpy.cu[prv]	低	该应用程序运行后监听用户短信，并上传到指定网址，会造成用户隐私泄露，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	GDI+ 远程代码执行漏洞（CVE-2020-0881）	高	Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。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[Banker]/Win32.Banker	中	此威胁是一种以窃取网络银行敏感信息 (如银行账号、密码、信用卡信息等）为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给黑客。
		Trojan/Win32.Sharik	中	此威胁是一种木马类程序。该家族通过映射内存的方式将自身注入的合法进程中运行，并添加注册表项实现自启动。该家族会主动连接远程服务器，接受攻击者命令。该家族还可会在电脑中下载、执行文件等。
		Trojan/Win32.Vobfus	中	此威胁是一种木马类程序。该家族运行后会修改注册表，阻止用户显示隐藏文件夹，连接网络下载其它恶意程序。该家族通常通过网络及可移动设备进行传播。
		GrayWare[AdWare]/Win32.HotBar	低	此威胁是一种可以推送广告的灰色软件家族。该家族样本运行后下载并安装推广应用，在用户浏览网页时可以弹出广告、占用系统资源、影响用户使用。
		GrayWare[AdWare]/Win32.Eorezo	低	此威胁是一种恶意广告木马类程序，可以在用户使用 IE 浏览器浏览网页时，弹出广告页面。该家族样本可能通过木马释放，运行后复制自身到系统文件夹下，修改注册表用以自启动。

为后新冠疫情时代的业务连续性保驾护航

杰森·阿尔伯克基 / 文 安天技术公益翻译组 / 译

这些基线业务连续性策略将有助于确保企业能够在业务环境发生变化的情况下保持正常运营。

在最近一段时间里，随着新冠病毒（COVID-19）传播所造成的影响进入到完全未知的领域，全世界每一家公司的优先事项都发生了巨大的变化。不光供应链和经济影响成为人们一直关注和担忧的话题，工作中断也成了令 CIO 和 CSO 头疼的问题，如果他们的员工不能外出，甚至不能到岗，他们将如何维持日常运营。

在冠状病毒活跃的地区，企业已经看到了这种影响。受感染的员工、高危人群以及可能与病毒携带者有过密切接触的人已被送往医院或被要求在家自我隔离。为了遏制“新冠”的传播，可能会很快关闭更多的学校和日托机构，这迫使一些父母在家照顾孩子几天、几周甚至更长时间。

有关疾病进展的最新消息不断出现，这使许多科技领导者感到焦头烂额。传统业务连续性关注点与疫情导致的业务连续性影响的关注点不同。传统上非常关注生产设施以及其具体场所导致的业务影响，而很少关注人员不能持续到岗造成的影响，而后者正是“新冠”疫情导致的影响。

为了应对“新冠”，人们做出了前所未有的努力，所有设施和学校系统都已关闭。为了帮助您克服由病毒引起的不确定性和焦虑，在您制定出流行病应对计划并使技术态势符合当前需求时，您可以优先采纳我们制定出的一些关键步骤。这些基线策略将有助于确保企业能够在业务环境发生变化的情况下保持正常运营。

现在的首要重点应该是构架您的商业弹性。“新冠”将对公司的日常工作造成严重破坏。适当的灵活性使得当惯常的运作模式改变时，也能保持正常运转；

要建立这种弹性，首先要对您的核心业务系统进行评估。大多数公司都有一个混合性的平台构架，有本地、云或者 Internet 模式，这种模式非常高效，而且成本较低，但是这种模式意味着必须开发一种工具，以确保员工即使在远程办公，也能够继续访问他们工作所需的工具和数据。

现在思考一下企业基础架构中有多少是位于本地的。如果冠状病毒的传播使得企业现场办公场所被关闭，或者，如果封闭的学校或隔离区等社区影响意味着员工将远程办公，团队将如何访问这些平台？需要考虑支撑所有员工远程办公的远程带宽，如果不足，需要及时增加；

还应考虑授权数量的增加，一些服务比如 VPN 以及其他软件存在授权问题。如果企业有1500名员工需要安全地接入网络，但只有 400 个 VPN 授权，那么能以多快的速度解决这一短缺问题，避免员工远程办公中断？防火墙的设置也需要相应更改，以适应增加的流量。IPS 设备还必须支持对非授权访问的拦截。这些 IPS 设备以及微分段必须一起计划。

不幸的是，黑客利用人们对“新冠”疫情的恐惧心理进行钓鱼活动，特别是假冒一些医疗卫生权威机构，这些活动已经非常猖獗了。非常时刻的员工，更容易受到攻击。企业的安全状况应包括对现有系统的审查，以便在钓鱼活动和其他入站威胁向量攻击员工的收件箱之前阻止它们，这样就不会在团队进行远程办公时试图阻止潜在的入侵。

对于小企业以及那些已经在为支持仓促准备的远程工作安排而努力的企业而言，即使执行这些核心步骤也可能是一个巨大的负担。

关键的第一步是审查组织机构的需求，并制定战略，以在快速变化的业务环境中以最佳方式促进沟通和协作。

下一步是制定短期战略，以最大限度地减少对运营的干扰，同时制定战略计划，以支持员工的潜在变化。

最后，必须评估并制定正确的长期方法，以确保现有或增强的业务连续性计划能够提供所需的弹性，这样在未来几周或几个月内，无论流行病会带来怎样的影响，组织机构都能灵活应对。请记住，在这个“新常态”中，唯一不变的是变化。唯一正常的事就是意外。

原文名称	Developing a Continuity Plan for the Post-Coronavirus World
作者简介	杰森 · 阿尔伯克基（Jason Albuquerque）。杰森 · 阿尔伯克基是 Carousel 公司的首席信息官和首席安全官。
原文信息	2020 年 3 月 16 日发布于 Information Week 原 文 地 址 https://www.informationweek.com/strategic-cio/it-strategy/developing-a-continuity-plan-for-the-post-coronavirus-world/a/d-id/1337293?
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。