我们用网络安全能力支持抗击疫情

安天应对新冠疫情应急指挥部

威胁框架：细粒度对抗

長纓待展

CONTENTS

目 录

智者安天下

威胁框架：细粒度对抗

01 利用新冠肺炎疫情相关信息的网络安全事件持续跟踪

联动守候与安全事件分析

应急响应时间轴

案例分析

利用疫情传播恶意代码的事件统计

面对疫情威胁的同时网络空间威胁不请自来

2009年攻击者利用H1N1疫苗接种主题的钓鱼邮件针对用户传播恶意代码

2009

2014

2014年犯罪团伙借助“埃博拉病毒”的信息“行骗”，针对关注埃博拉病毒的用户进行钓鱼邮件攻击

2015年网络攻击者借中东呼吸综合征（MERS）在韩国肆虐期间开展网络攻击活动等

2015

2016

2016年网络犯罪分子使用Zika（寨卡）病毒为题的钓鱼邮件针对一家医疗保健提供商传播勒索软件

- 此类事件往往借助用户对疫情的恐慌心理而盲目点击各种信息
- 远程办公缺少足够安全保障等提高网络攻击的成功率

- 主要攻击方式为邮件钓鱼攻击

  假新闻链接：虚假的链接为挂马网站

  恶意附件：附件为恶意的样本实体

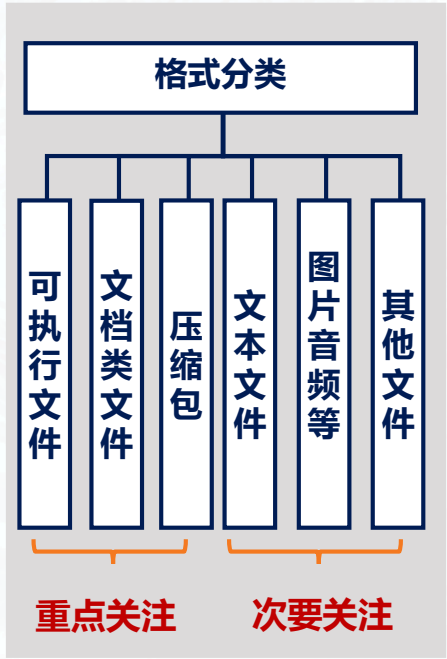
安天CERT的联动守候与事件分析的工作安排

疫情关键字守候

疫情 新增病例 N95 Wuhan 疫情防控 钟南山 Coronavirus 李兰娟 新增病例 逃离武汉 复工 卫健委 COVID-19 肺炎 口罩 小汤山 隔离 疫苗 火神山 新冠 发热

守候结果

样本格式分类输出



分析流程

重点分析

第一时间上报与发布

风险分析

分类- 根据事件进行分类

风险分析-样本功能与危害分析

事件评估

研判影响-研判事件影响上报有关部门

发布风险分析与防护建议报告

智者安天下

威胁框架：细粒度对抗

应急职守团队全面跟踪分析、上报、发布等工作响应

专家团队应急值守

7*24小时应急响应

梳理有关事件

针对事件类型
分类、梳理、汇集

公众发布报告

疫情防控期的几类网络安全威胁分析与防范建议

入选工信部疫情防控重点保障单位

重要事件持续跟踪与上报

安全事件全面跟踪

针对疫情相关的事件，启动持续跟踪分析与研判

报送有关部门

安天向有关部门报送安全事件列表以及相应的风险分析

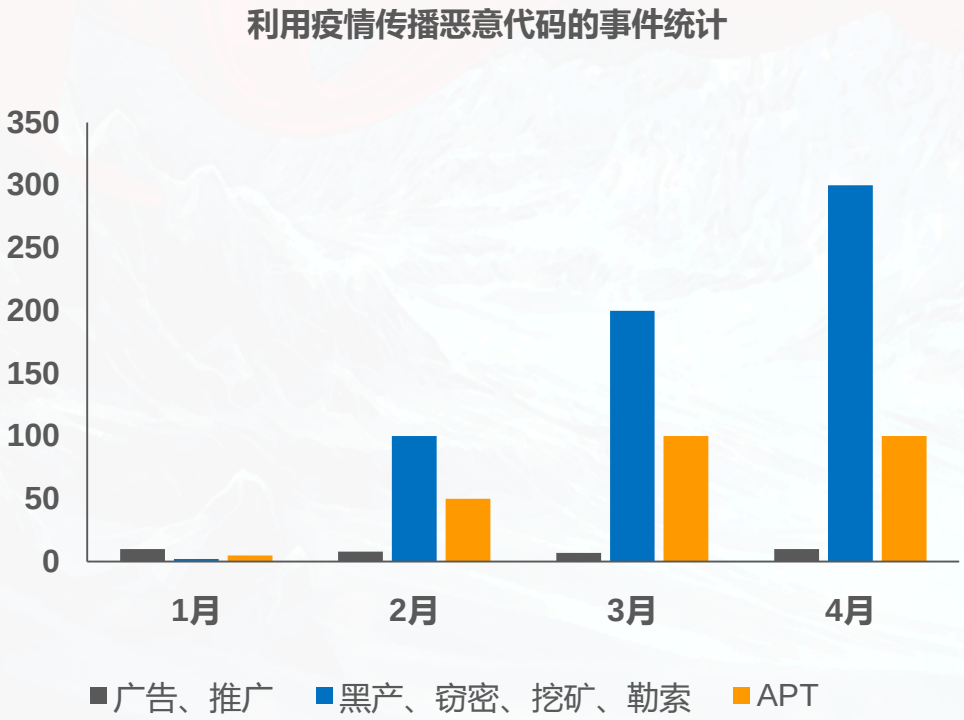
事件简报报送

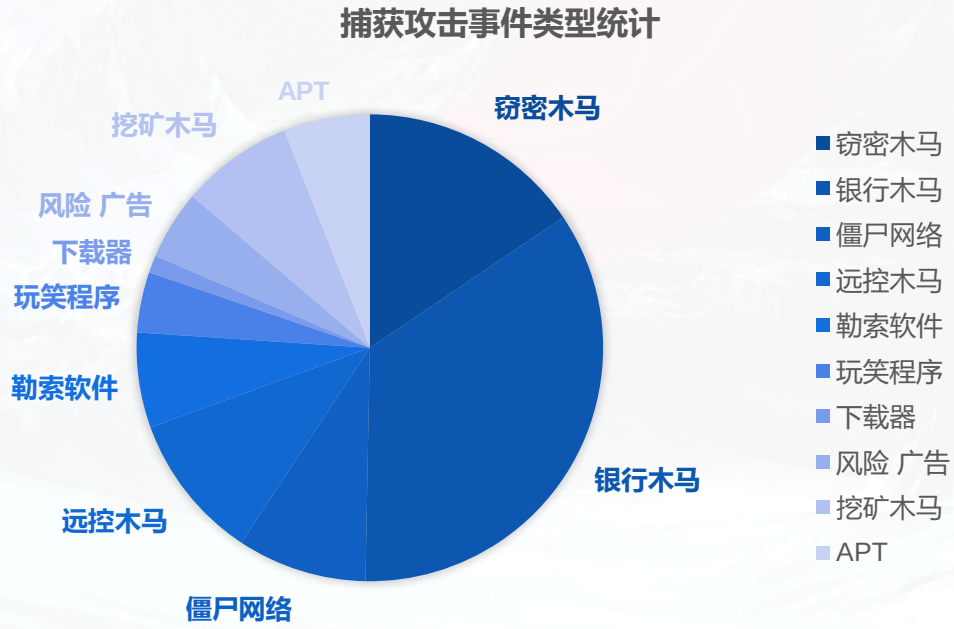
中心以及有关主管部门（阶段性）

APT、黑产等事件

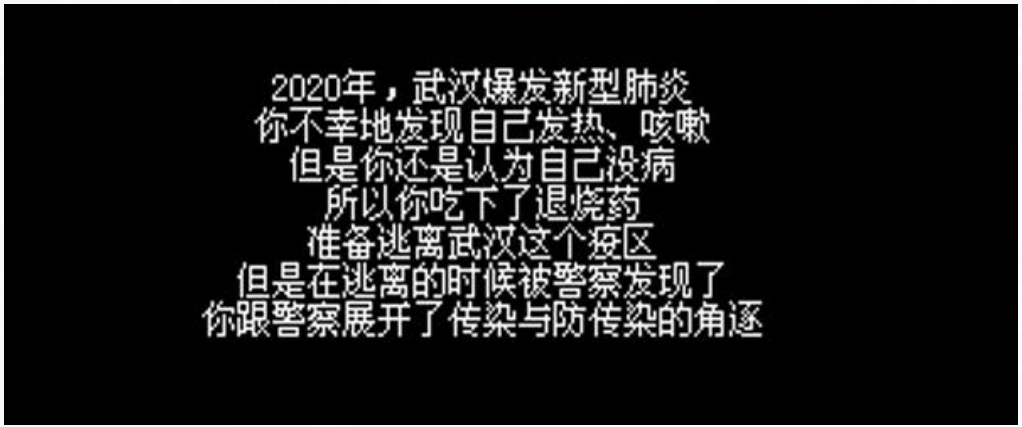
安天向有关部门汇报安天跟踪的针对我国实施APT、黑产等攻击事件

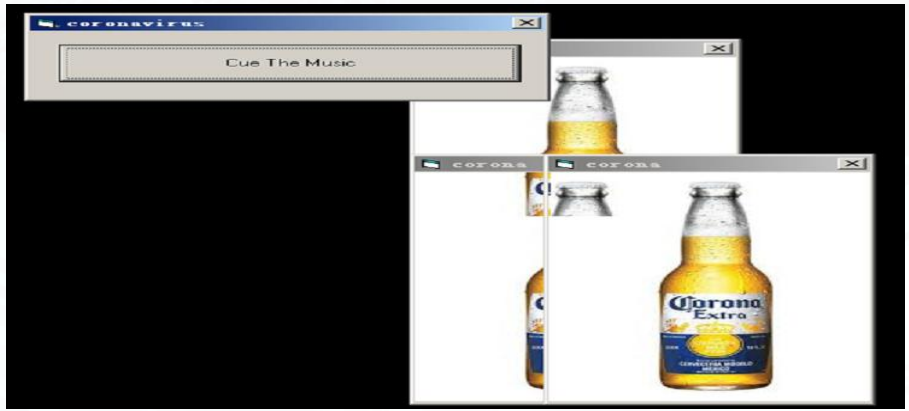
利用疫情信息传播恶意代码统计





无实际危害的恶作剧类程序



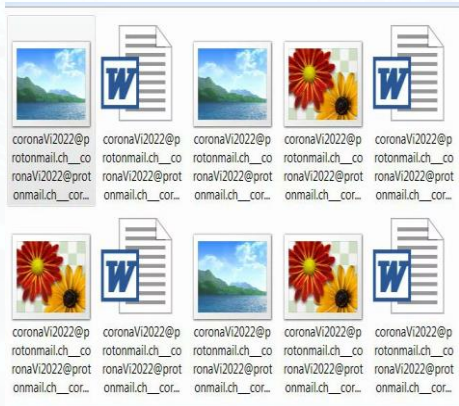


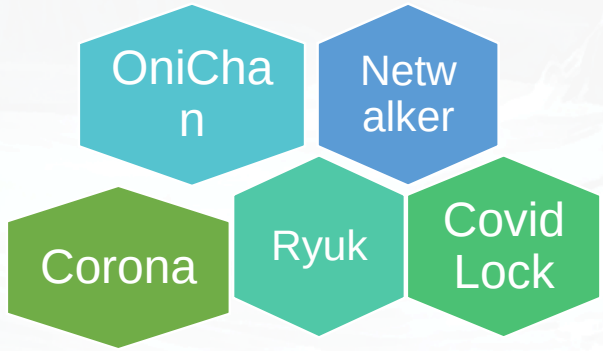
勒索软件组织趁火打劫

2020-02-13日，捕获到首个达摩勒索软件案例，借疫情相关信息作为传播内容，勒索信内容中攻击者使用“coronavirus@qq.com”作为联系邮箱，而“coronavirus”翻译为中文则是“冠状病毒”

《传播CoronaVirus勒索软件和KPOT窃密木马事件的分析》

多个勒索利用疫情信息传播





Emotet大范围传播窃密样本

安天CERT从2020年2月17日至18日间，监测到数十个使用相同文件名“n Wednesday, China reported far fewer cases of the novel coronavirus”且哈希值不同的相似样本，多个样本大小一致，编译时间多数在“2020年2月14日20时27分至28分“左右，通过对恶意样本的深度关联与分析，判定该恶意代码为Emotet银行木马

利用疫情信息文件名：
n Wednesday, China reported far fewer cases of the novel coronavirus.doc
周三，中国报告的新型冠状病毒病例少得多

白象组织利用疫情相关信息对我国发起针对性攻击

案例一

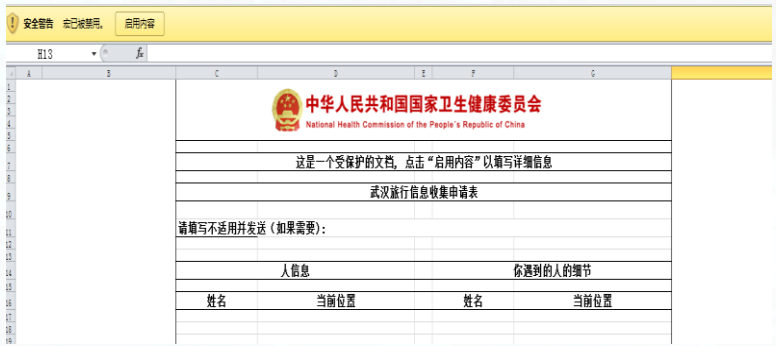
- 伪造官网： http://nhc-gov.com/h_879834932/
- 诱饵文件： “卫生部指令.docx”
- 伪造成“中华人民共和国国家卫生健康委员会”

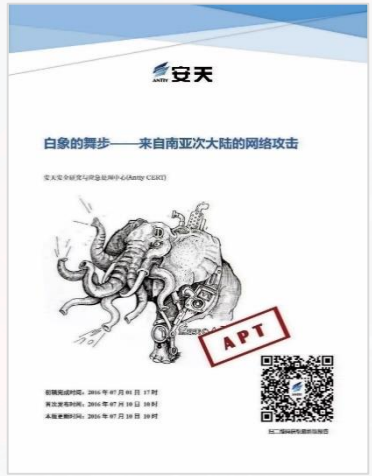
一旦攻击目标点击“提交”按钮，便会连接C2下载白象木马加载器

案例二

- 伪造官网： http://nhc-gov.com/h_879834932/
- 诱饵文件：武汉旅行信息收集申请表.xlsm
- 嵌入了恶意宏代码，启用后会通过“scrobj.dll”

调用远程sct文件，sct 代码继续从服务器中下载伪装成 jpeg 文件的可执行后门文件。

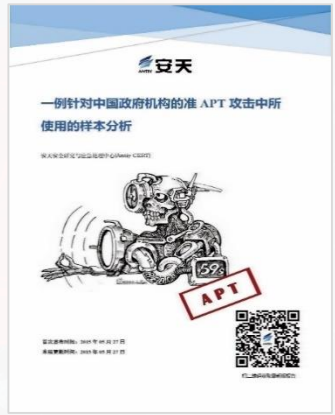




APT-TOCS（海莲花）、绿斑组织针对我国实施网络攻击

钓鱼邮件攻击

钓鱼网站攻击



02 疫情期间网络安全现状风险分析

疫情下远程办工以及数据泄漏的风险分析

邮件仍是攻击者最常用的攻击入口

疫情下远程办工以及数据泄漏的风险分析

终端脆弱性

远程办工的终端通常没有企业网络健全的多防御体系，而很有可能成为攻击者窃取内网的跳板。

通信方式的安全性

企业VPN、远程登陆、会话软件、企业通讯平台等通信方式的多样化导致攻击面的扩大。

敏感数据泄露

多数使用个人电脑、智能手机、平板等设备等方便携带的同时也极易丢失，一旦设备遗失，可能导致重要数据泄漏。

公民信息

出于疫情防控需要而采集的公民个人信息，可能被不当利用

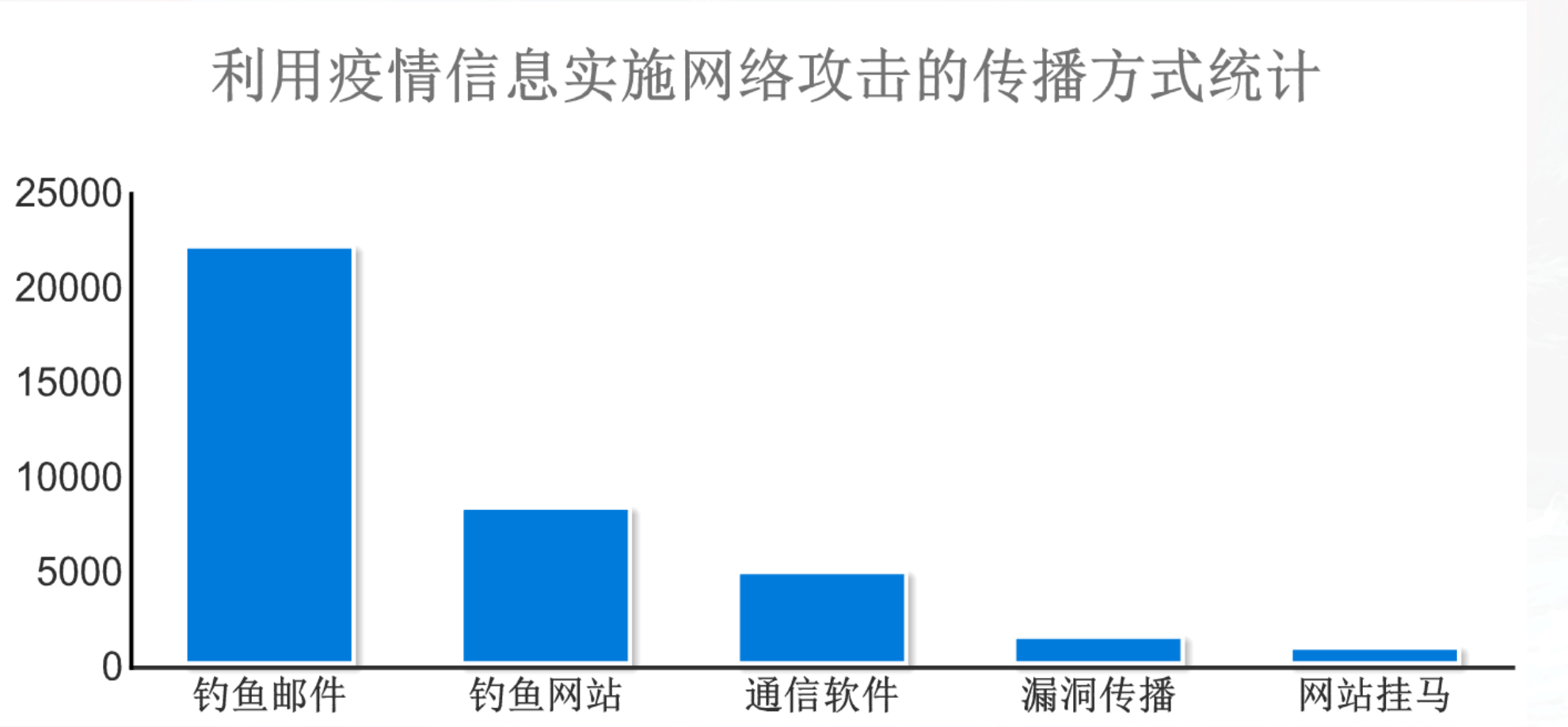
案例：今年7月重庆某地冷冻链一厄瓜多尔白虾成核酸阳性，此时某营销公司却将一份名为《重庆已购进口白虾顾客名单》公布在其公众号供下载。该名单包括原告赵某在内的重庆各区县一万多名购买进口白虾人员的姓名、家庭住址、身份证号码、手机号码等详细个人信息。最终被法院判处赔偿。

敏感数据泄露

医院、卫生机构、疫苗组织的相关数据在攻击者眼中具有很高的价值

- 欧洲药品管理局遭黑客攻击 涉及辉瑞新冠疫苗关键数据
- 俄罗斯黑客涉嫌大规模窃取疫苗数据
- 黑客在欧洲窃取了辉瑞/BioNTech COVID-19疫苗数据

邮件仍是攻击者最常用的攻击入口



03 战疫情——安天在行动

安天推出一系列力所能及的举措

安天·移动安全免费开放智信——零信任移动安全接入服务

疫情期间 提供智信零信任移动安全接入的免费服务

在零信任安全架构基础之上，云管端协同联动，为企业建立一套完整的虚拟安全边界并提供更加安全的应用访问环境。

零信任策略优化平台

智信应用安全交付网关

智信安全工作空间(SDK)

零信任应用安全访问


用户接入区
智信应用安全交付系统
业务服务区
移动终端业务接入
PC业务接入
IOT业务接入
国密TLS
统一身份认证
终端状态感知
智信安全工作空间（SDK）
零信任策略优化平台
动态访问控制
动态访问控制
终端安全 数据安全
信誉评估 策略计算
应用/API
安全代理
身份安全 链路安全
应用安全交付网关
用户行为感知
数据交互感知

智信 安全工作空间和安全交付网关

专家团队24小时应急响应

专家团队24小时值守

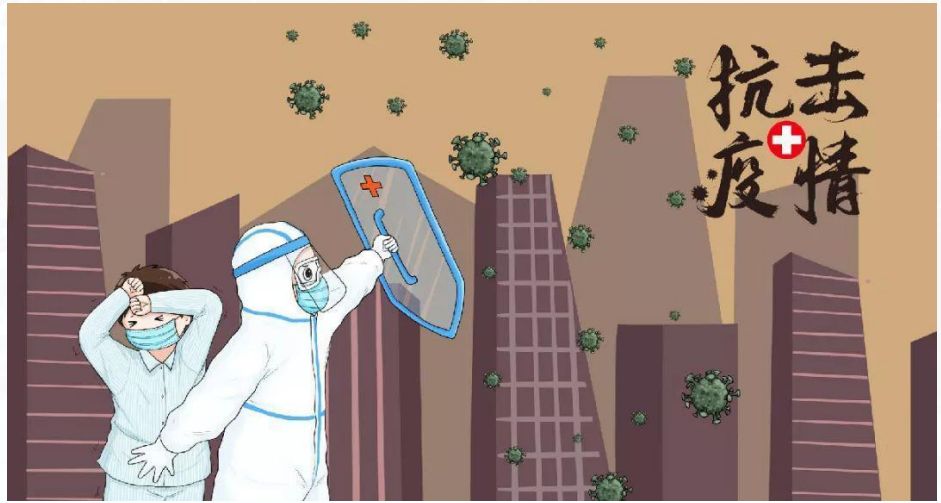
- 安天客服热线已经由客服值守改为专家团队值守
- 为全国医疗卫生系统提供免费安全咨询和应急响应服务

应急服务方式

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！

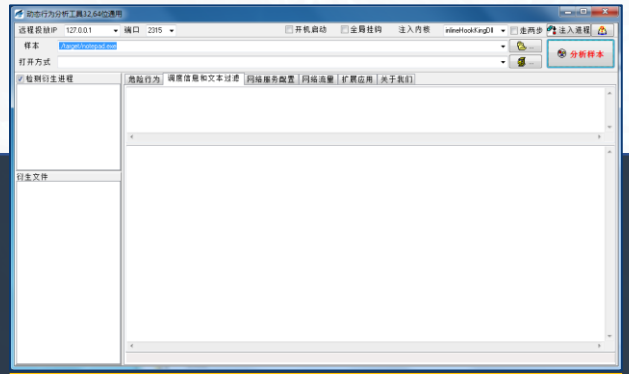


23 廿九	24 除夕	25 春节	26 初二	27 初三	28 初四	29 初五	30 初六	31 初七	1 初八	2 初九	3 初十
武汉封城				因疫情延长假期					专家团队24小时值守		

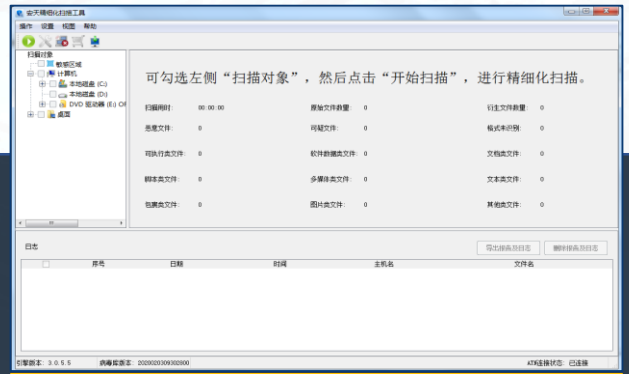
免费开放安天安全工具——疫情免费版

发布三款工具免费版本

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。



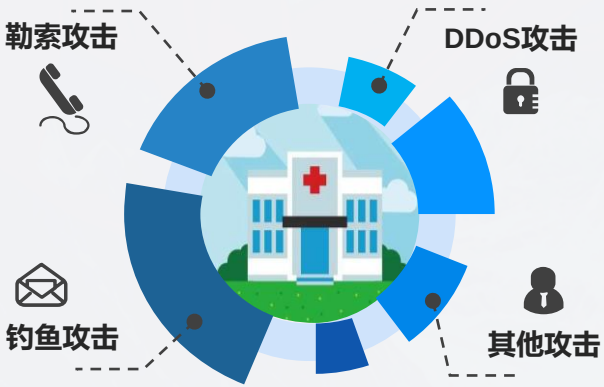
Action Scope 轻量级文件行为分析工具



Scan Tool精细化扫描工具

Atool系统安全分析工具

免费开放安天智甲——医疗定制版



医疗行业火力集中

医疗行业是重点保护对象，
也是火力集中的地

医疗行业重点保护

一旦遭受类似勒索这种低成本，
高破坏的攻击，后果不堪设想

- 迅速响应疫情对医疗行业的核心保护需求，第一时间向新冠定点医院免费开放两年期医疗特别定制版。

- 安天智甲终端防御系统，基于多年的勒索病毒行为特征的积累，构建了一个具有强大分析与判断能力的勒索病毒行为特征库，可有效针对医疗行业防勒索以及其他攻击。

安天智甲
ANTIY 医疗版-疫情保障专版

04 安天公益研发

机构人员分布和返程分析工具

背景介绍

新型冠状病毒肺炎疫情爆发后，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。安天希望能利用公司可视化技术为抗疫出一份力。

万家团圆时，将士未下鞍。年初五开工，于2月3号早8点发布，免费面向社会、面向机构企业使用，目前，全国已有多家机构正在使用中。

23 廿九	24 除夕	25 春节	26 初二	27 初三	28 初四	29 初五	30 初六	31 初七	1 初八	2 初九	3 初十
武汉封城				因疫情延长假期		开工					发布

需求分析

国家疫情数据感知

全国范围内，动态展示按行政区划分的疫情感知

个人健康数据感知

个人出行及健康数据，对个体范围内展示的疫情检测

企业复工数据感知

?

23 廿九	24 除夕	25 春节	26 初二	27 初三	28 初四	29 初五	30 初六	31 初七	1 初八	2 初九	3 初十
武汉封城				因疫情延长假期		开工					发布

智者安天下

威胁框架：细粒度对抗

需求分析

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，做好复工的准备与保障和员工的返程安排。

人员分布

春节假期，员工分布在全国各地，甚至在国外，掌控员工坐标

返岗情况

全国各地员工计划返岗时间、返岗路线、所乘交通工具等信息记录

企业复工数据感知

健康情况

远程每日更新员工健康状况，掌握员工是否有健康异常

隔离情况

因疫情延长假期，在家隔离并实施远程办公，根据防疫政策更新功能

23 廿九	24 除夕	25 春节	26 初二	27 初三	28 初四	29 初五	30 初六	31 初七	1 初八	2 初九	3 初十
武汉封城				因疫情延长假期		开工					发布

工具简介

安天的安全工程师应急编写的“机构人员分布和返程分析工具”，所提供的工具包名称为“Antiy_SAT”，本工具旨在帮助各单位在疫情期间梳理员工的健康情况和节后返岗情况，掌握员工在全国动态分布情况，为各单位在安排好人员返程和复工方面，提供一定的保障。

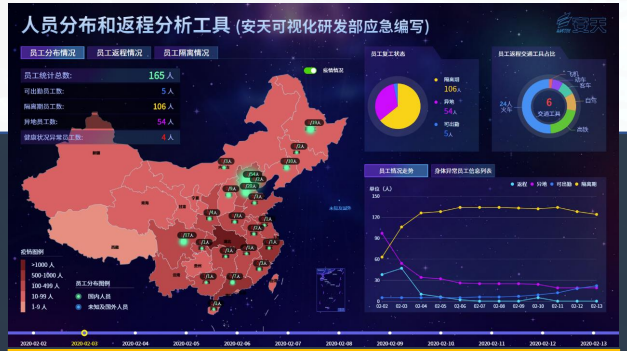
数据安全与隐私

考虑到相关人员信息的敏感性，安天特别将本工具开发为完全的本地化工具，
数据处理和可视化分析呈现都在使用者的主机上进行，保证了各单位数据的隐私和安全。

工具功能介绍

工具模块

安天开发的“机构人员分布和返程分析工具”，共分为三部分，分为员工分布情况、员工返程情况和员工隔离情况三个模块，每各模块的内容都可以通过最下方的时间轴对数据进行筛选。

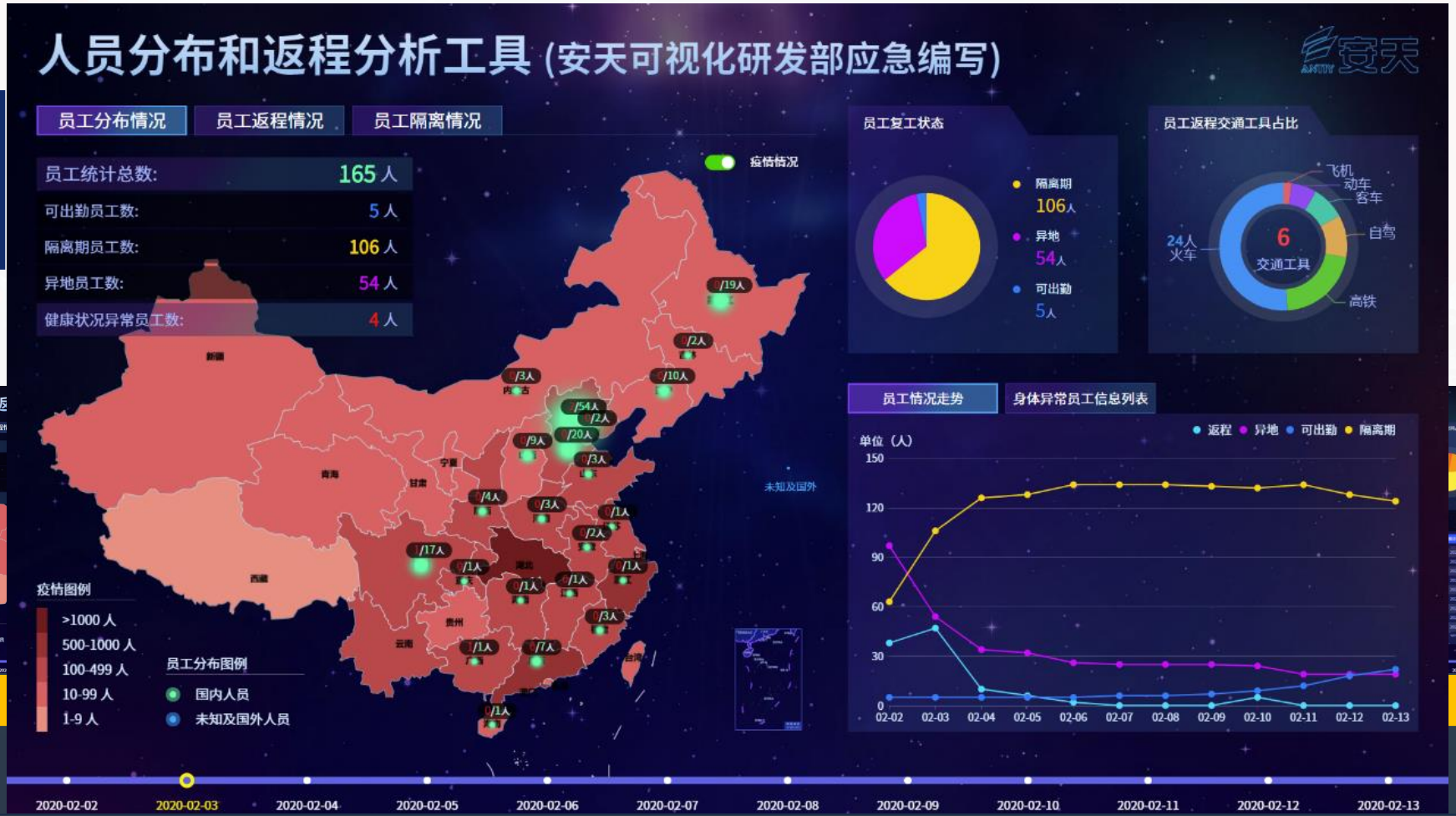


员工分布情况

员工返程情况

员工隔离情况

工具功能介绍


人员分布和返程分析工具 (安天可视化研发部应急编写)
员工分布情况
员工返程情况
员工隔离情况
员工统计总数: 165 人
可出勤员工数: 5 人
隔离期员工数: 106 人
异地员工数: 54 人
健康状况异常员工数: 4 人
疫情情况
疫情图例
>1000 人
500-1000 人
100-499 人
10-99 人
1-9 人
员工分布图例
国内人员
未知及国外人员
未知及国外
员工复工状态
隔离期 106人
异地 54人
可出勤 5人
员工返程交通工具占比
6 交通工具
飞机
动车
客车
自驾
高铁
24人 火车
员工情况走势
身体异常员工信息列表
返程 异地 可出勤 隔离期
单位（人）
150
120
90
60
30
0
02-02 02-03 02-04 02-05 02-06 02-07 02-08 02-09 02-10 02-11 02-12 02-13
2020-02-02 2020-02-03 2020-02-04 2020-02-05 2020-02-06 2020-02-07 2020-02-08 2020-02-09 2020-02-10 2020-02-11 2020-02-12 2020-02-13

工具功能介绍

工具功能介绍

成果与反馈

对内

- 安天作为首批复产复工的企业，小工具为防疫期间安天内部开展工作提供了便利。
- 对异地员工数、员工健康与隔离状况、异常员工数、返程员工数等指标进行大数据分析，综合梳理筛选员工的健康数据和节后返岗情况，助力安天安全有序复工复产。

浏览量：

10万+

下载量：

千余次

对外

- **审计署 等多个部委和政府机构；中国航油等多家企业；湖南大学 等多所高校**使用了本工具，下载量达到数千次，获得各界广泛好评。
- 小工具发布后，在部分行业和客户中得到应用，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，并根据客户需求做了二次开发，不断的更新完善。

致谢

开源工具库：

"tweenjs/tween.js": "^17.3.0",
"axios": "^0.18.0",
"d3": "^5.9.1",
"echarts": "^4.6.0",
"element-ui": "^2.5.4",
"jquery": "^3.3.1",
"three": "^0.101.1",
"three-css3drenderer": "^1.0.1",
"three-orbitcontrols": "2.101.1",
"three-subdivision-modifier": "^1.0.5",
"vue": "^2.6.6",
"vue-router": "^3.0.1",
"vuex": "^3.0.1"

字体：

思源黑体 CN Light
思源黑体 CN Regular
思源黑体 CN Bold

本工具在开发过程中，用到较多开源工具库和字体，在此对以上开源工具库和字体的作者表示感谢。

2020社会责任榜 —— 安天

- **2020年2月，安天入选了工信部疫情防控重点保障企业名单。**
- 2020年10月，《2020中国互联网企业社会责任报告》考察的18个互联网行业，240个分析对象中：
  安天位列网络安全行业第一名。
- 安天将继续承担起网络安全企业的责任与担当，赋能客户，共筑网络安全防线。

23 廿九	24 除夕	25 春节	26 初二	27 初三	28 初四	29 初五	30 初六	31 初七	1 初八	2 初九	3 初十

武汉封城　　因疫情延长假期　　启动安天应急值守制度

战疫情 安天人在行动

中国的抗疫是医生、护士、警察、海关、街道社区、各行各业的无数抗疫民众组成了一道防疫屏障，阻挡了疾病的蔓延，每个人都是战士，每个人都是英雄。

网络安全的保卫中，安天人用技术为网络安全打造了一道防护墙，阻挡了威胁的蔓延，保卫网络空间的安全与健康。

战疫情，安天人在行动！

谢谢大家