疫情期间网络安全如何“免疫”攻击

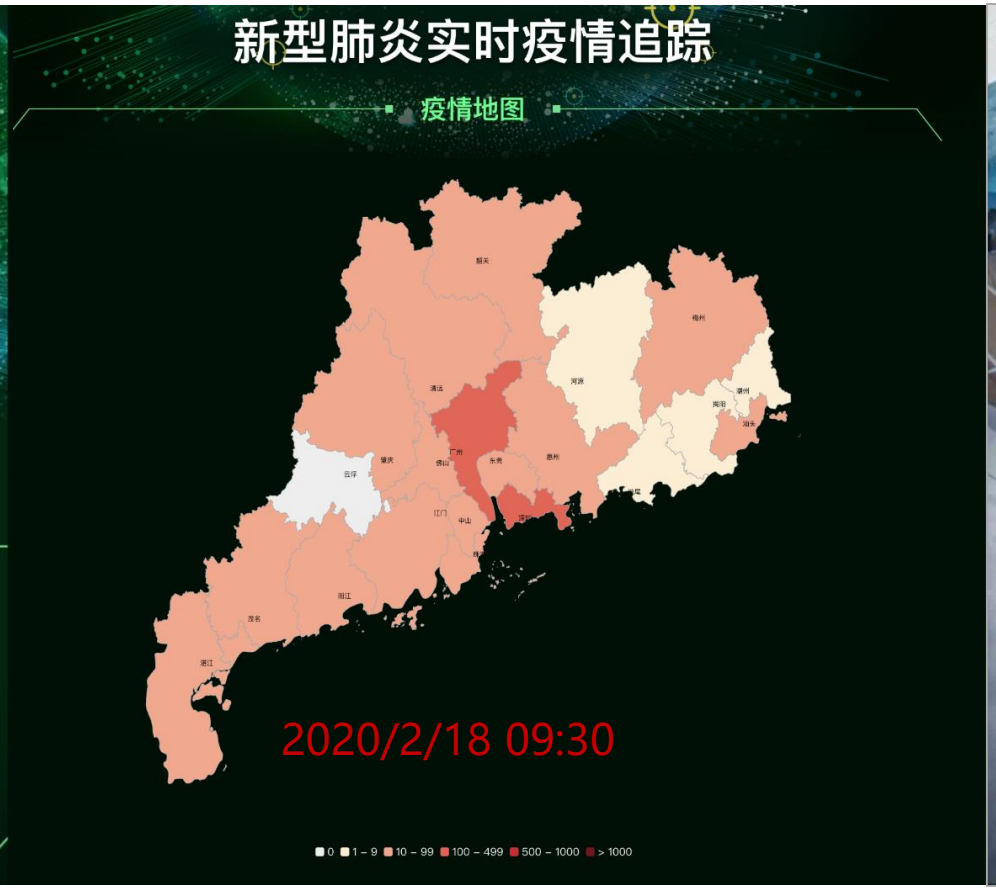
陈辉

时间:2020/02/15

目　录

Contents

疫情严峻、全国一心



全国疫情依然严峻

听党统一指挥，减少外出，就是最大的贡献

做好宣传和舆论引导，群防群治，打赢关键战役

◆ 2020新年伊始，全国范围内大面积爆发新型冠状病毒肺炎疫情。目前，疫情传播还没有阻断，疫情防控进入关键时期，**疫情信息公开透明**，引导舆论，群防群治，及时把握**疫情防控态势**，是做好防控病毒的基础。

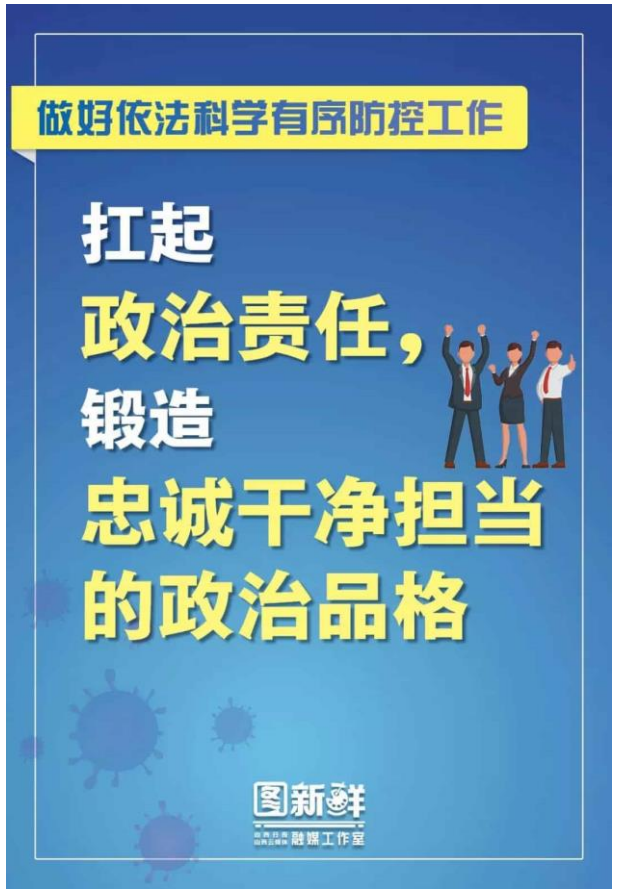
中共中央政治局常务委员会2月3日会议

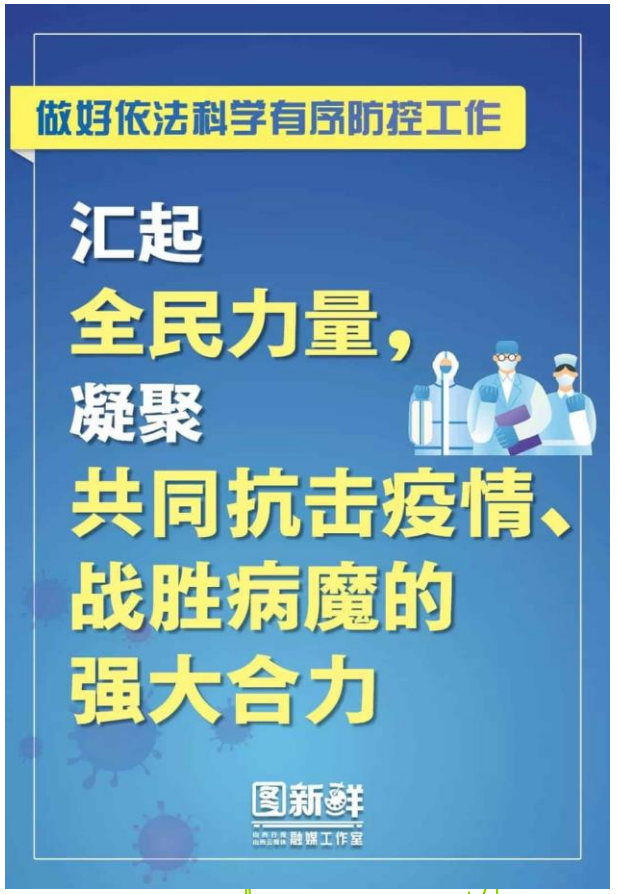
◆ **习近平指出，要做好宣传教育和舆论引导工作，统筹网上网下、国内国际、大事小事，更好强信心、暖人心、聚民心。**

- 充分报道各地区各部门联防联控的措施成效，生动讲述防疫抗疫一线的感人事迹。
- 加大对传染病防治法的宣传教育，引导全社会依法行动、依法行事。
- 正视存在的问题，及时发布权威信息，回应群众的关切，增强及时性、针对性和专业性，引导群众增强信心、坚定信心。
- 加强对健康理念和传染病防控知识的宣传教育，教育引导广大人民群众提高文明素质和自我保护能力。

习近平指出要全面提高依法科学防控依法治理能力

各级政府要坚持依法防控治理，做到科学精准有效，在最吃劲关头守住底线攻城拔寨。

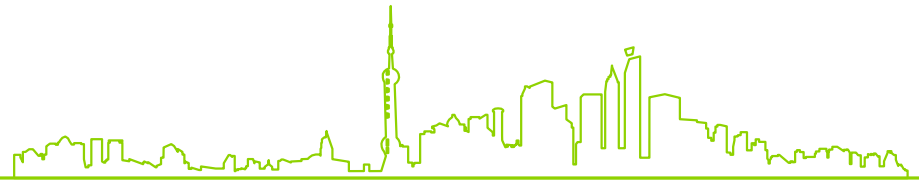




政府当前重点工作


当前工作5重点
加强
医用物资
生产采购调度
当前工作5重点
帮助
中小微企业
渡过难关
当前工作5重点
保障
农业生产
不误农时
当前工作5重点
抓好
经济运行调度
当前工作5重点
做好
一线先进典型
宣传报道

为什么当灾难来临时,总是多事之时。



是真相还是谎言

各国对生物战都讳而不言 但不能以阴谋论视其为无物|人... 新浪军事

7天

场

疫情是生物战争?彭光谦将军:组建生物国军_西陆网

1天前

智库理

专家:无明确证据证明板蓝根对预防新型冠状病毒有效--人民... 人民网

2020

主要

"武汉将断网以禁止医务人员分享信息"系谣言_通信_搜狐

2020年

相关信

北京协和医院辟谣"肺炎患者出逃":仍在治疗|北京协和... 新浪新闻

"造谣"8人之一的李文亮医去世,中央派人到武汉调查:真相到底是...

1天前

等8人

口罩股和"双黄连"概念股走高,谁是疫情下的资本赢家?

5天前

概念

新型冠状病毒与SARS基因组序列80%相似究竟意味什么_发现频道_中国...

2020

分类。

疫情谣言一网打尽NO.15:武汉市卫健委某领导感染后逃往上海

4天前

擅离职

武汉医院走廊尸体无人处理!真相曝光!

2020年1月26日 - 一"武汉市红十字会医院",是当地患者家属也是个护士,医院内因为医疗物资严重不足情况已经失控,甚至有三具尸体就和病人们一起停留在走廊上,无人处理。...

警惕：一系列电脑版“新型冠状病毒”正在悄然蔓延

“新冠病毒”一：远程控制 窃取文件

“新冠病毒”二：删除文件 电脑变砖

“新冠病毒”三：黑产不休 变招作祟

以下为疑似该电脑病毒的部分列表，收到后切勿点击：

- 深圳发现今年首例赛卡病例，该旅客从柬埔寨归国！.exe
- 今晚菲出现购口罩狂潮，商店门口围满了人.exe
- 新型冠状肺炎袭击菲律宾，已确诊病例七人.com
- 帕塞带孩子女性疑似新型病毒感染被当街暴打.exe
- 逃离武汉.exe
- 新型冠状病毒肺炎病例全国已5名患者死亡；警惕！！.exe
- 冠状病毒.exe
- 新型冠状病毒预防通知.exe
- 双重预防机制.scr
- 新型冠状病毒感染的肺炎防控工作指挥部令.exe
- 新型冠状病毒肺炎.exe
- 疫情防控投入.exe
- 新型冠状病毒预防通知.exe
- ……

疫情期间的网络安全事件

- 疑似台湾绿斑黑客团伙的虚假“疫情统计表格”和“药方”!
- 那个借新型肺炎对我国发起攻击的黑客组织叫印度“白象”!
- 境外黑客扬言将攻击我国视频监控系统!
- 南亚APT组织借新冠疫情对我国医疗机构发起定向攻击!
- .....

这是现阶段普遍存在的三种攻击情况:

- 以疫情关键字为诱导的病毒钓鱼攻击
- 以疫情为诱饵的信息泄露导致的诈骗攻击
- 以疫情捐赠为由的携善款跑路的诈骗攻击

疫情期间网络安全相关的政策法规

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
WWW.CAC.GOV.CN
请输入检索关键词
首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题
当前位置：首页 > 正文

拔除网络生态“杂草”——《网络信息内容生态治理规定》今年3月1日起施行

2020年01月20日 11:07 来源：人民日报海外版 【打印】【纠错】

当我们借助互联网的便利自由浏览阅读免费、快捷、海量的网络信息时，网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等行为也在污染着网络生态。针对这些问题，国家互联网信息办公室近日发布《网络信息内容生态治理规定》（以下简称《规定》），自2020年3月1日起施行，旨在营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益。

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China
WWW.CAC.GOV.CN
请输入检索关键词
首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题
当前位置：首页 > 正文

2020年防控新型网络安全风险将成为重中之重

2020年01月19日 16:05 来源：新华网 【打印】【纠错】

新华网北京1月19日电 17日至18日，中央政法工作会议在京召开。记者从会上获悉，2020年要把防控新型网络安全风险摆在突出位置来抓，提升网络社会综合治理能力，不断健全网络社会综合防控体系。

一是构筑打击遏制网络犯罪的“新高地”。要抓住群众反映强烈的网络贩枪、网络黄赌毒、网络传销、电信网络诈骗、网络套路贷等新兴网络犯罪，完善线索快速落查、跨区域协作和跨境执法司法合作机制，深化打击整治行动，坚决打掉网络黑灰产业链，遏制网络犯罪高发势头。

二是构筑大数据安全的“防护罩”。要把大数据安全作为贯彻总体国家安全观的基础性工程，依法严厉打击侵犯公民隐私、损坏数据安全、窃取数据秘密等违法犯罪活动。

三是构筑新业态风险的“隔离带”。要坚持鼓励创新与确保安全相统一，对新技术、新产业、新业态、新模式，既留足发展空间又坚守安全底线。（记者 卢俊宇）

疫情期间网络安全相关的政策法规

近期网安部门通过网络安全监测发现多起利用新型冠状病毒肺炎疫情等相关题材，冒充国家卫健委、疫情防疫等部门，向部分单位及用户投放与新型肺炎疫情相关的钓鱼邮件，并利用钓鱼邮件进行病毒传播、网络攻击的行为。黑客组织利用新型冠状病毒疫情，制造传播一系列计算机病毒，这些病毒文件名均带有"冠状"、"病毒预防"、"肺炎病例"、"逃离武汉"、"新型冠状肺炎"等热门字样。病毒通过邮件、社交网络等方式传播，社交网络为病毒传播的主要传播渠道，感染后可导致计算机被远程控制、信息被窃取等危害。目前，病毒正通过社交网络蔓延。

钓鱼邮件常常附带恶意链接与包含恶意代码的office文档附件，利用仿冒页面实现对用户信息的收集，诱导用户执行恶意文档中的宏，向受害用户主机上植入木马程序，实现远程控制和信息窃取。

防范建议如下：

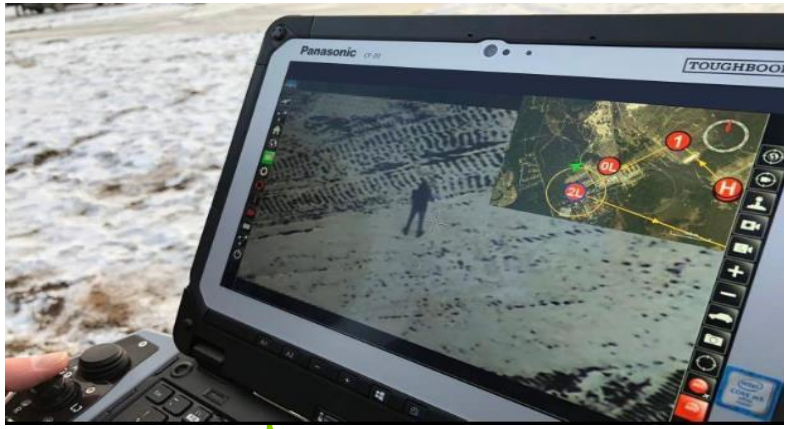
- 收到和疫情相关的邮件，特别是邮件内带有附件或带链接的需要特别注意，若遇到 exe 文件、包含未知文件的压缩包文件等，不点击打开。
- 关于疫情相关的文章，需确认是否为国内权威媒体及正规网站，不轻易打开非官方权威媒体发布的文件、文档，不盲目转发非权威媒体公布的链接及文件。社交网络转发的文件、图片等，打开前先进行病毒查杀。
- 电脑设备须安装正规杀毒软件，及时更新病毒库，做好系统补丁升级。
- 不要启用Office宏，除非文档来自可信来源。

新挑战

新的时代、新的机遇、新的契机、新的挑战

美欧多国密集开展网络演习，网络演习走向常态化

序号	演习名称	时间
1	五眼联盟“网络夺旗”演习	2019年6月21日至28日
2	美欧举办多国网络演习“军刀卫士19”	2019年6月3日至24日
3	美国防部组织“网络闪电2019”演习	2019年3月13日至26日
4	美陆军举办“2019网络X-Game”演习	2019年6月7日至16日
5	欧盟举办首届“Blue OLEx 2019”网络演习	2019年7月2日至3日
6	英20家高校参加“水星训练（Exercise Mercury）”网络演习	2019年1月
7	北约组织“锁盾2019”网络安全演习	2019年4月9日至12日
8	欧盟为2019选举进行网络安全演习	2019年4月5日
9	美陆军组织“网络盾2019”网络演习	2019年4月5日至20日



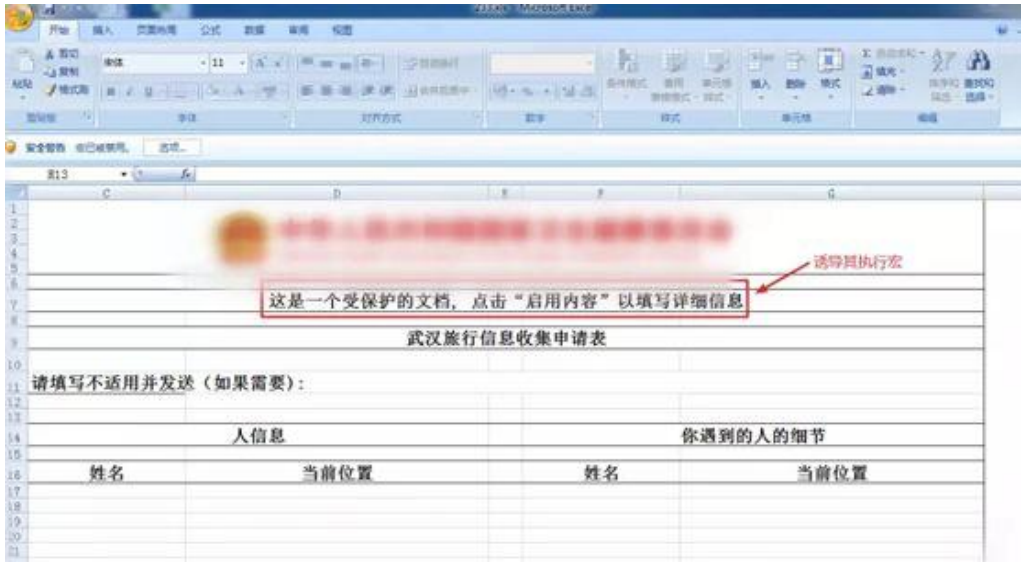
疫情亦网情

360安全大脑捕获印度APT组织对我国医疗机构发起定向攻击！

就在全国人民万众一心抗击疫情之时，360安全大脑捕获了一例利用新冠肺炎疫情相关题材投递的攻击案例，攻击者利用肺炎疫情相关题材作为诱饵文档，对抗击疫情的医疗工作领域发动APT攻击。

文件名	MD5	安装者
新型冠状病毒感染引起的肺炎的诊断和预防措施.xlsm	[redacted]	[redacted]
武汉旅行信息收集申请表.xlsm	[redacted]	
收集健康准备信息的申请表.xlsm	[redacted]	
申请表格.xlsm	[redacted]	[redacted]

新冠病毒之后网络空间成疫情战役的又一重要战场。



该攻击组织使用采用鱼叉式钓鱼攻击方式，通过邮件进行投递。公然利用当前肺炎疫情等相关题材作为诱饵文档，部分相关诱饵文档如：**武汉旅行信息收集申请表.xlsm**，进而通过提示诱导受害者执行宏命令。

简单说，攻击者其将关键数据存在worksheet里，worksheet被加密，宏代码里面使用key去解密然后取数据。然而其用于解密数据的Key为：nhc_gover，而nhc正是中华人民共和国国家卫生健康委员会的英文缩写。

疫情期间，警惕电信网络诈骗新套路

一.购物类诈骗

方式1 虚假售卖口罩等防疫物资

诈骗分子利用大家急于购买储备N95/医用口罩等防疫物资的焦急心理，谎称有货或者可以帮忙代购，在受害人付款后，找理由拒不发货或直接拉黑失联，骗取钱财。

方式2 利用钓鱼购物网站虚假销售诈骗

诈骗分子利用疫情热点，搭建钓鱼购物网站，通过虚假售卖口罩、药物等方式，引诱受害人点击钓鱼链接，填写个人敏感信息，借此盗取受害人信息或个人财产。

方式3 网络刷单诈骗

诈骗分子利用疫情发生以来，大量民众"宅在家中"的情况，通过发布"足不出户，工资日结，工作轻松，报酬丰厚"等刷单广告，实施网络刷单诈骗，引诱受害人刷单付款后，拒不退款，骗取钱财。

小编反诈提醒

1. 购买口罩、酒精、消毒液等防护用品或药品一定通过正规渠道。
2. 不要点击来源不明或陌生号码、网站发送的网址、链接，不要随意泄露、填写个人敏感信息，尤其是银行账户密码、手机验证码等信息。
3. 网络刷单不可做，宅在家中莫被骗。

二.退改签/退费诈骗

方式1 火车票/飞机票退改签诈骗

诈骗分子利用疫情期间，国内、国际部分交通停运、变更的情况，通过发送虚假的火车票、机票退改签信息，引导用户点击诈骗网址或拨打虚假"客服电话"，收集受害人银行账户、密码、手机验证码等重要信息，盗取用户钱财。

方式2 旅游/酒店/快递退费

诈骗分子利用疫情期间，大量旅游及酒店的预定行程取消及快递发货困难的情况，以押金返还、快递退费为借口，发送虚假信息，引导用户提供银行账户、密码、手机验证码等重要信息，盗取用户钱财。

小编反诈提醒

1. 退改签、退费不需要提供银行密码和手机验证码等信息，如果对方要求提供此类信息，一律拒绝。
2. 通过官方渠道办理火车票、机票退改签及酒店、快递退费等业务。
3.要加强个人信息保护，不轻易填写敏感个人信息。

三.冒充类诈骗

方式1 冒充政府部门，推销"特效药"

诈骗分子利用大家对疫情的恐慌心理，通过假冒政府部门、疾控部门或者相关药物研究部门推广所谓的防治新型肺炎"特效药"、"新药"、"国外药"，骗取购药钱财。

方式2 冒充亲属，谎称新型肺炎感染诈骗

诈骗分子冒充受害人亲属，谎称受害人子女或其他亲属突然高烧，已被隔离医治，利用受害人焦急心理，要求对方立即汇缴"住院费"等，骗取钱财。

方式3 冒充慈善机构，骗取爱心捐款

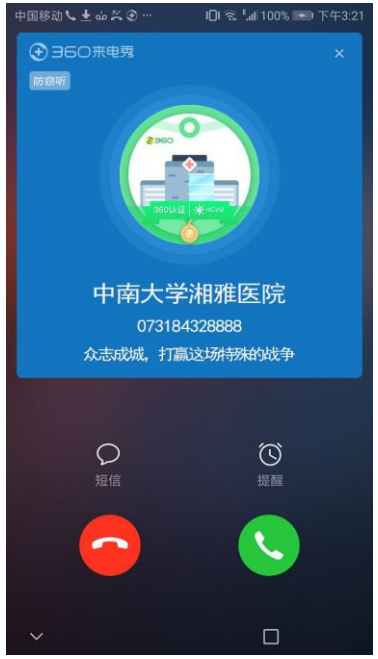
诈骗分子利用疫情期间，大家共抗新型肺炎疫情的爱心和同情心，发送"献爱心"的虚假信息，骗取民众爱心捐款。

小编反诈提醒

1. 请严格遵医嘱用药购药，对在宣传中使用"特效药"、"新药"、"国外药"等字样的，要提高警惕，以免上当受骗，守护好自身的财产安全。
2. 收到亲属被感染的信息不要惊慌，要通过电话和网络等多种方式验证确认，不要轻易给陌生账户打款。
3. 请通过正规渠道进行爱心捐赠，捐赠过程中不要提供银行密码及手机验证码等重要信息。

“疫”号码通防欺诈

面向各类企业与机构，战“疫”号码通，通过对企业机构的官方电话号码等信息的认证、识别和在用户接听时的号码标记，提高用户电话接听率，满足疫情期间企业机构与大众的电话通讯需求。目前，战“疫”号码通中，已涵盖医院类、疾控中心、卫健委、心理咨询、投诉维权等板块，合计近三万通讯号码。



在战“疫”号码通中，企业机构可自行提交名称、所在区域、所属行业等相关信息，申请认证。完成认证后，当机构拨打用户手机时，**即可在用户手机的来电界面中展示机构信息，包括：Logo、名称及联系电话号码。**

而360手机卫士的十亿多大众用户，则可通过战“疫”号码通对企业机构的认证标识，**避免错过电话联络，或遭受电话欺诈和隐私泄漏**

移动办公“金钟罩” 护航政企移动业务安全

移动办公金钟罩其基于移动零信任模型+企业移动数据DLP防泄漏+360移动大数据威胁情报三板斧，为企业移动业务安全保驾护航，全面赋能企业移动业务的移动环境安全，移动数据安全以及移动行为安全。

体系化防护移动业务安全

企业移动业务安全整体安全，是动态的安全，防护对象应涉及移动业务的相关载体，人，设备，网络，业务自身以及载体之间的行为，防御手段应做到**事前感知防御，事中响应，事后审计，**

实时感知动态决策，精准识别安全风险，准确定级危害程度，精细化决策安全防护策略新一代基于人工智的安全解决方案

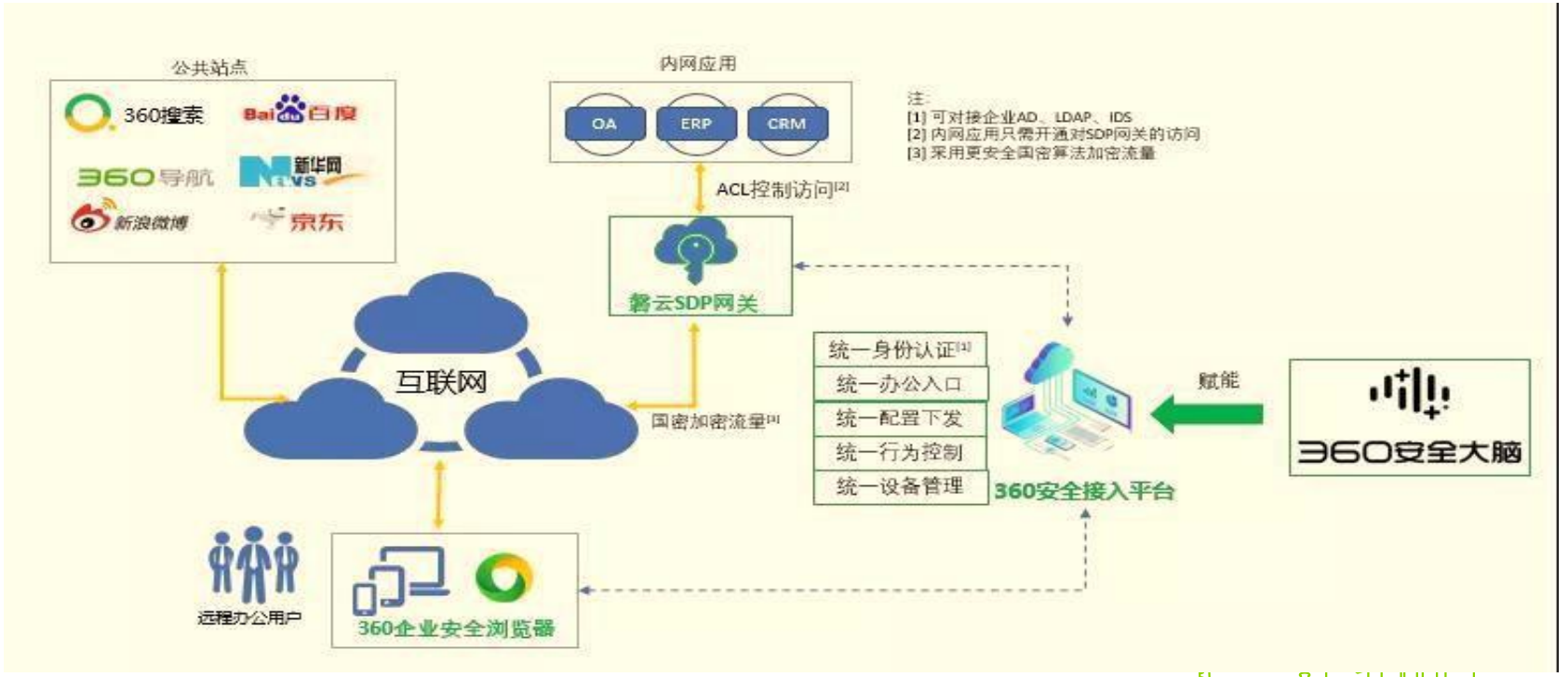
精细化决策移动业务安全响应策略

依托360大安全体系联动分析协同运营

基于大安全协同体系，保障全面安全而非局部安全，整体安全而非个体安全，动态安全而非静态安全，主动安全而非被动安全，才能打好企业安全，国家安全，网络安全这场真正的阻击战

远程办公“云盾甲”防护

在疫情防控期间，依托磐云安全防护系统及企业浏览器，为各政企单位提供SDP（软件定义边界）解决方案，可帮助各级政企单位内部员工在远程办公的过程中，**隐藏核心网络资产与设施**，使之不直接暴露在互联网下，使得网络资产与设施免受外来安全威胁。



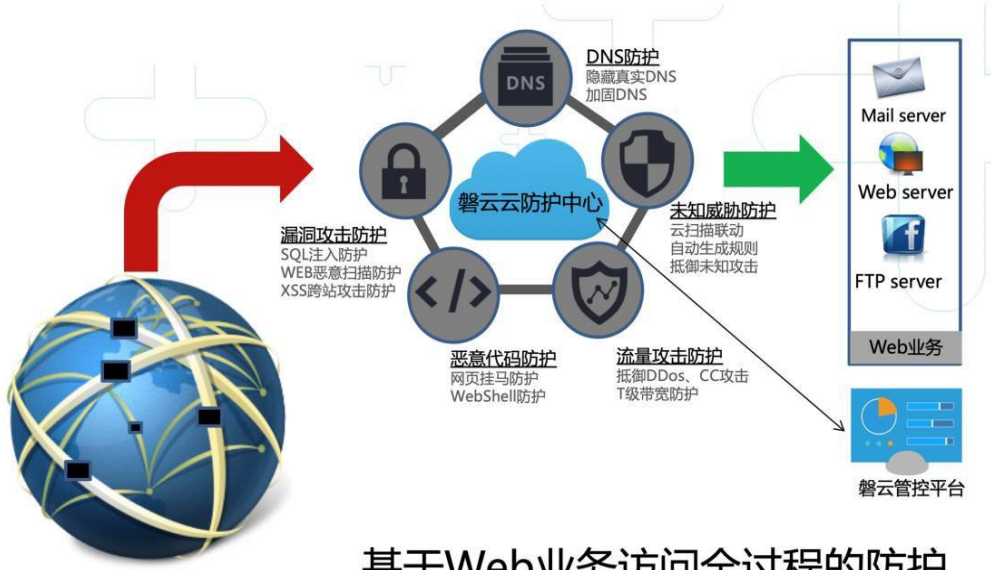
网络安全问题的本质是bug

Web业务监测防护服务

针对疫情期间黑客利用对病毒恐惧传播木马病毒，360集团在疫情期间提供免费WEB业务监测防护服务，可通过SAAS服务远程接入云探和磐云服务，提供7*24小时100%准确率的风险告警，为医疗单位、政府机构、防疫救灾部门及各大企事业单位的网站稳定护航。

三六零云探

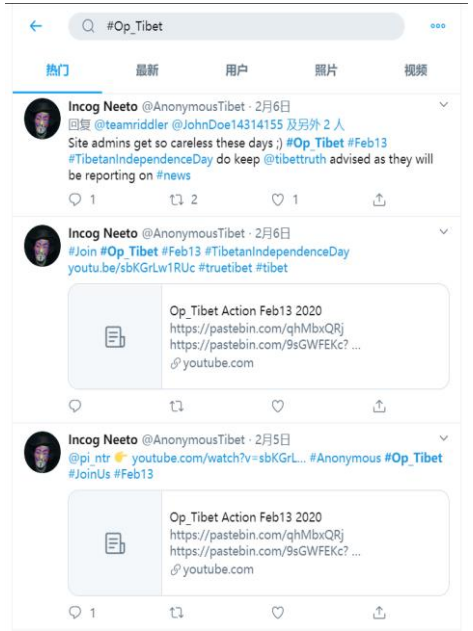
三六零磐云



基于Web业务访问全过程的防护

视频监控系统案例

2020年2月，360CERT团队通过360安全大脑监测发现，近期有境外黑客组织发布推文，扬言将于2月13日对我国视频监控系统实施网络攻击破坏活动。该组织声称已掌握我境内大量摄像头控制权限，并在平台公布了70余个闭路电视系统外围探测信息。360物联网安全团队第一时间回应事件，为广大用户及物联网设备厂商支招。



网络资产风险监测

疫情期间，面向所有企、事业单位及政府监管单位免费开放360巡天平台（一站式工业企业资产网络安全风险探测平台），工业互联网安全疫期专项技术支持团队。平台将在第一时间帮助接入单位定点排查安全隐患，从资产探测、漏洞扫描、数据查询、数据分析展示等全维度展开安全服务工作，帮助各企业加强生产网络及办公网络安全防护能力。

疫情期间，360巡天平台具体将提供以下安全服务：

- 提供工业互联网综合安全事件分析与宏观安全形势报告；
- 总体安全态势呈现，帮助企业及时规避、封堵风险隐患，保障安全有序生产；
- 精准辨识、定位暴露在互联网上的工控系统设备，无损发现设备漏洞、风险；
- 支撑监管单位完成安全监测、检查、整改的闭环工作；

生物病毒与计算机病毒在特点、防范方面的共同点

	新冠病毒	勒索病毒
特征	感染人	感染电脑和文件
	破坏免疫力，严重的要命	影响使用，严重的毁坏数据，勒索要钱
	潜伏期一般在1-14天	潜伏期不定
组织措施	断路，阻止病毒携带者进入	断开网络
	封城，封社区	根据业务情况设置不同的安全域，通过防火墙限制各安全域的访问
	非指定人员不得出入	网络和主机准入，未经允许的主机和用户不允许接入网络，未经允许的进程不允许运行
	进城进小区要量体温，疫区返乡人员隔离观察	设置防火墙策略，关闭不必要的端口将可疑流量转入EDR和KATA产品中进行分析。
	关闭海鲜市场，分析病毒源，追溯可能的接触者	发现电脑中毒不要急于恢复系统镜像，通过安管平台（SIEM和SOC）收集报警信息和日志信息，进行取证分析，追溯病毒来源和感染路径
	通过电视、手机、传单等方式全方位宣传病毒情况和感染方式	开展网络安全知识讲座，提高网络安全意识，增强网络安全技能，养成良好的使用习惯。
	科研部门分析病毒研发疫苗	漏洞修复，升级病毒库
	公开透明，及时通报感染人数与感染方式，通过感染热点区域分析，感染人群分析，病毒分析，提前做好预警	利用威胁情报，配合其他安全措施，对要害区域及早防控
个人措施	不要吃野味，容易感染病毒	不要使用盗版或者来源不可靠的软件
	人人戴口罩	每台电脑安装防病毒软件
	不要串门、少聚会、做好个人消毒	设置个人防火墙，关闭非必要端口，共享文件夹进行严格权限和进程访问管控，并执行审计，不要乱点邮件，乱上网
其他	全社会休假，医务工作者一线拼死奋斗	安全运维全天候奋力值守
	太平盛世容易忽略医务工作者的重要性	风平浪静时容易忽略安全运维的价值
	感染后无特效药，人死不能复生	备份是唯一的救命药，有备份就有可能恢复。应重视数据和应用系统备份

计算机病毒只是一个程序或者代码，之所以叫他病毒，就是 因为他具有同医学病毒相似的属性。 对于病毒的概念，准确说应该叫恶意代码，是指能够引起计 算机故障，破坏计算机数据，影响计算机系统的正常使用的 程序、代码、指令。 生物病毒具有破坏性、潜伏性、传染性、隐蔽性、非授权性、不可预知性。计算机病毒同理，在入侵计算机后，也会对 计算机和网络进行破坏、会隐藏系统中不会马上发作、并且 具备自我复制传播或者通过其他途径进行传播的能力、无需

系统管理者授权对计算机进行无感知的破坏。

病毒木马查杀

已知病毒木马

采用云查杀机制，文件信誉引擎（全球最大）

双静态查杀引擎，双静态病毒库

未知病毒木马

人工智能查杀引擎：QVM-II（国际专利）

虚拟执行沙箱引擎：QEX

文件运行跟踪引擎：主动防御（RTE）

特种病毒木马

私有云白名单模式

非白即黑的强安全管理策略

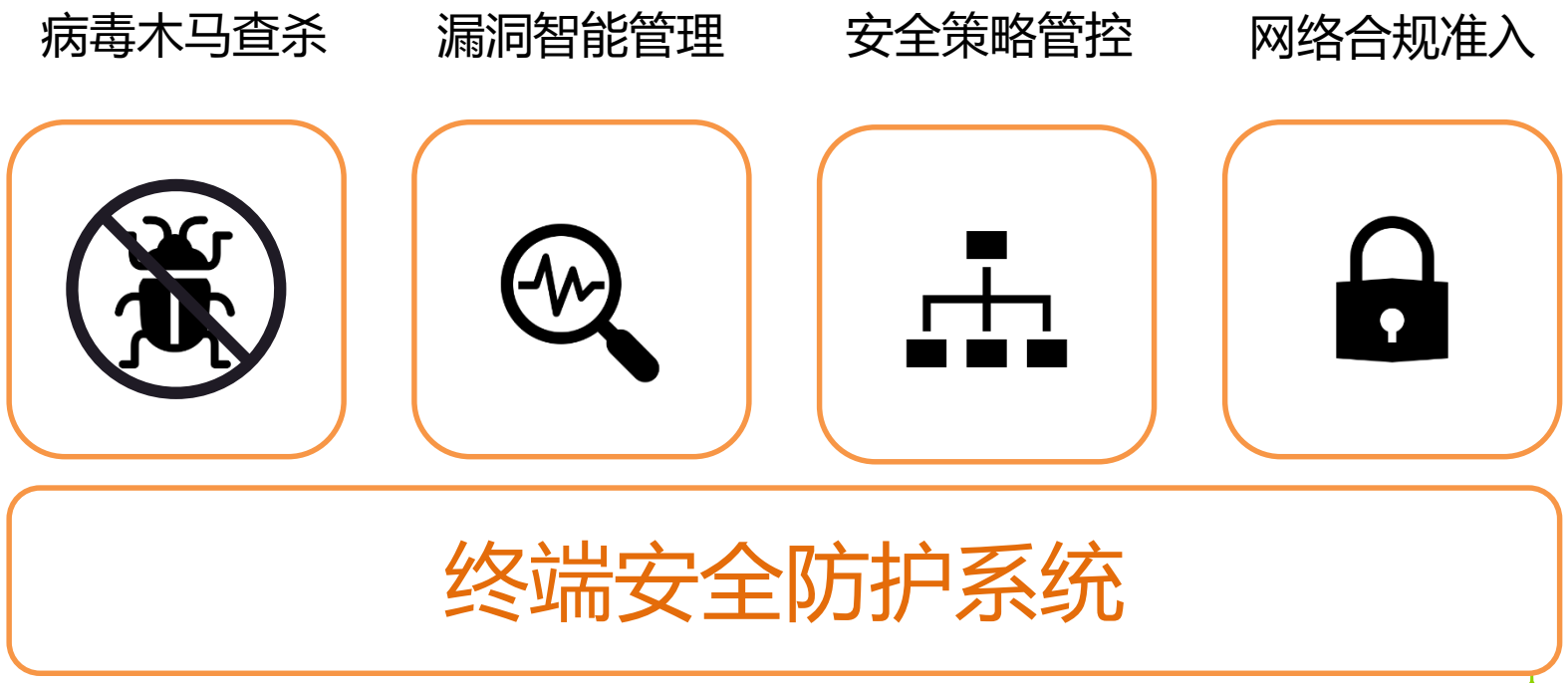
安全加固

恶意URL信誉引擎（国内最大）

多层应用防火墙立体防护

终端安全防护

- 插件化，安全防护与管控模块按需使用
- 防护与管控“All in One”解决方案



WIN7停护 盾甲来保障

就在微软宣布**Windows 7系统停服**前夕，一场前所未有的0day漏洞组合攻击正伺机引爆，全球首例同时复合利用IE浏览器和火狐浏览器两个0day漏洞的攻击风暴悄然突袭。近日，360安全大脑就全球**首家捕捉到此次攻击**，并将其命名为**“双星”0day漏洞攻击**。

Windows 7系统正式停服，正如曾经Windows XP系统，其背后必然酝酿着未知且重大的网络安全风暴。由于官方停止对Win7系统的防护，各类型网络攻击势必接连涌现，在漏洞百出的Win7系统大肆作恶。

360 Win7盾甲由网络安全防御智能的雷达系统360安全大脑重磅打造，以360安全大数据为基础，综合威胁情报、知识库、安全专家的各项能力，全力构建微补丁漏洞免疫，以及再度升级的系统核心加固、关键程序保护、防护日志四大核心功能，为国内近6成用户继续护航Windows 7系统的安全。

Win7停服引爆网络暴击国内超六成用户曝光在“双星”漏洞阴霾之下

机遇

一棵树长得越高，它的根就需要扎得更深

机遇

2003年非典没有击溃阿里，反而成就了电商行业。

2020年新冠将促使互联网深化
网络安全企业将越显重要
但大安全、泛安全将更重要

一线抗疫的排头兵

- 1月27日，国家卫生健康委召开新闻发布会。
- 国家卫生健康委疾病预防控制局一级巡视员贺青华表示，**社区是实施网格化管理的基础，是传染病防控的第一道防线以社区防控为重点**，切实落实综合防控措施，做到“早发现、早报告、早隔离、早诊断、早治疗”，将有效地遏制疫情扩散和蔓延。

防控任务艰巨

全国多个疫情严重区域都采用严格隔离措施，隔离后监管、信息收集、疫情排查，社区管理人员压力巨大。

严格控制出入的政策，传统基层人员值守，增加了管理人员的接触风险。

上门调研信息、查控疑似隔离人员，让基层管理人员疲惫不堪、接触传染风险增加。

360企业安全集团第一时间上线疫情专题

360旗下产品360搜索、360快资讯、360浏览器、360手机卫士等，迅速整合平台资源，上线抗疫专题，24小时迭代更新，提供最迅捷、全方位、多层次疫情信息获取和求助服务。

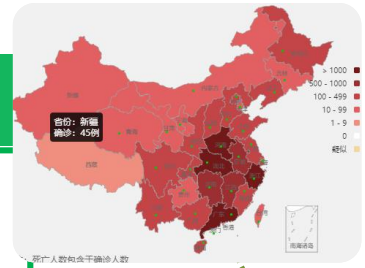
面对2020年春节期间爆发的新型冠状病毒肺炎疫情，360集团公司各主体和周鸿祎个人累计筹集近**1亿元**资金，通过360基金会全部购买了各种医疗物资送到疫区。

疫情防控手段需升级，统筹线上线下，打赢关键战役

指挥

看不清、听不畅、判不准

人力物资有限，难以实时把握疫情动态，无法有效根据根据疫情部署针对性的防控措施



执行

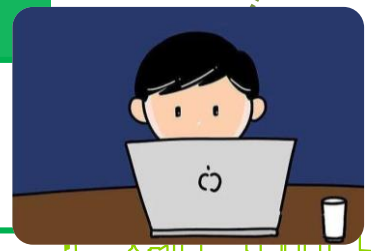
数据汇总难、及时响应难、执行跟踪难

缺乏有效的管控措施，辖区情况难摸清，外来人口难核对，多头上报，效率低，疲于奔命

群众

内心不稳、求助不畅、真相难辨

群众隔离在家易焦虑，急于了解疫情信息，需要有线上反馈和服务求助渠道



360城市安全，基于大数据助力科技战“疫

全方位| 全在线| 最迅捷| 全智能| 多层次

社区居民数据
病患个人信息
病患轨迹信息
武汉返回人员信息
互联网舆情信息
政策法规信息
……

线索上报
疫情分析
信息发布

疫情大数据分析


信息在线发布


病患关系挖掘


疫情态势分析

区域疫情展示
疫情信息上报
患者同程查询
在线公共服务

防疫后台管理
疫情智慧研判
每日疫情研报
病患轨迹呈现
…

多维呈现

公众版
民众
政府
专业版

公众版：实时疫情发布，便捷线上服务，满足群众需求，维护区域稳定

专业版：智能分析研判，助力政府把握疫情态势，实现疫情精准防控

360 “科技战疫”产品及服务概览

社区疫情防控

360人工智能人脸识别、语音机器人工智能物联网助力社区封闭信息化管理

运程安全办公

360云计算、云存储、云直播让远程协同工作更轻松

疫情指挥中心

360大数据可视化、大数据辅助决策助理疫情指挥调度

安全全程保障

360安全大脑时刻保护网络、数据安全
IOT安全保护移动、物联网终端安全

新的战场、新的要求

实战是检验安全能力的唯一标准

威胁	防御手段	防御武器	
外网：已知漏洞利用、显性攻击... 内网：违规行为、数据窃取	筑墙	边界安全	合规体系
	层层设防	主机安全、系统安全、应用安全	
外网：零日漏洞利用、APT攻击、网络武器.... 内网：数据泄露、供应链漏洞、社会工程学....	发现（大脑）	攻防知识体系 深度情报分析 零日漏洞挖掘专家	实战体系
	实战对抗	攻防武器体系 专家赋能平台	
	即时响应	作战指挥平台 快反应急体系	

安全大脑自顶向下赋能

神经元（传感器）

安全产品

深度防御产品

第三代产品（实战安全、能力输出）：
EDR、NDR、xDR、NTA、蜜网/欺骗防御……

第二代产品（合规/应用安全）：
NGFW、WAF、……

第一代产品（合规/被动安全）：
FW、IDSP、终端杀毒……

合规安全产品

安全服务

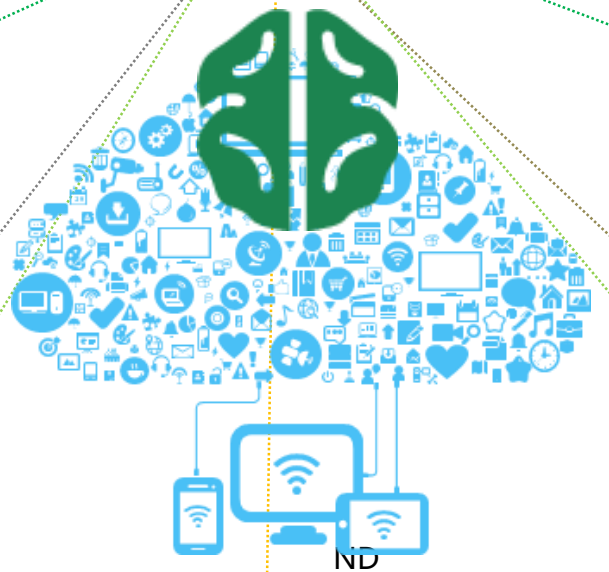
实战安全服务

第三代服务（实战化服务、XaaS服务）：
网络战、护网、攻防演练、XaaS、MSSP……

第二代服务（合规/分级安全）：
等保分保、合规要求、安全培训……

第一代服务（合规/日常运维）：
安全巡检、驻场运维……

合规安全服务



EDR　NDR　CDR

基础设置

端&系统	网络	云&应用
PC、手机、IoT泛终端	互联网、专网、5G	私有云、公有云、混合云、分布式云

业务场景

关键基础设施　政务云/产业云　传统互联网　工业互联网　产业互联网　智慧城市

应对网络战/APT威胁/实网攻防：体系化协同作战能力

协同联动体系

360安全大脑

知识云
漏洞云 情报云

分析云
查杀云 沙箱云

专家云
培训云 实战云

9朵云

威胁情报平台 | 智能分析平台 | 专家协同平台

3平台

神经元网络

1套神经元网络

360网络安全大脑

不是单纯的技术产品
而是360安全能力赋能平台

=

实战安全体系赋能平台

知识赋能基地

- 网安学院
- 科普基地
- 双创基金库

产品支撑体系

- 安全运营中心
- 实网攻防产品
- 实战攻防靶场
- 关基合规产品

服务支持体系

- 安全运营服务
- 安全运营工具
- 专家赋能服务

领域纵深体系

- 国家安全
- 城市区域/行业安全
- 政企安全

3层防线

应对网络战/APT威胁/实网攻防：技术创新能力

技术创新能力

国家新一代人工智能
开放创新平台

十二个安全研究中心

360 Vulcan team
360 QVM团队
360 SkyGo team
360 天马团队
360 Cole team
360 追日团队
360 手机卫士安全研究团队
360 0Kee团队
360 Vulpecker team
360 Unicorn team
360 Nirvan team
360 Marvel team

四大开放平台

猎网平台
网络安全研究院
补天漏洞响应平台
360威胁情报中心

四个创新实验室

360人工智能实验室
360冰刃实验室
360安卓安全生态实验室
360网络攻防实验室

关键词：**安全研发年投入25亿元**

亚太地区最大的安全创新中心
覆盖网络安全完整技术生态

应对网络战/APT威胁/实网攻防：大网的“一手”情报

大网的“一手”情报， 大数据能力

TOP 1
最大的
程序文件样本库

总样本数**180亿**
每天新增**900万**样本

每天300T+数据

TOP 1
最全的
行为日志库

总日志数**22万亿**条
每天新增**380亿**条

103亿条记录

TOP 1
最大的
存货网址率

每天**800亿**次活跃网址访问记录

141款产品

TOP 1
最全的
全球域名信息库

每天分析**2000亿**条次DNS解析记录
全球**80亿**域名信息

12亿+覆盖用户

关键词： **109个数据中心，25万台服务器**

应对网络战/APT威胁/实网攻防：顶级攻防专家能力

蝉联世界攻防大赛Pwn2Own全球总冠军

各类顶级攻防大赛冠军

- 2019 MSRC全球最具价值安全精英榜中，360凭借超强的实力封神屠榜，夺得亚洲首冠，排名全球第一！这也是有史以来中国人首次问鼎！
- 360公司共有10人荣耀登榜，其中7人皆在榜单前50。无论入选人数和综合排名，360均位列世界第一，成为2019 BlackHat当之无愧的“头号赢家”。
- 来自360Vulcan Team的古河、招启汛包揽前两名。招启汛还荣膺有“全球白帽黑客奥斯卡”The Pwnie Awards支撑的大奖“最佳提权漏洞奖”，一举打破了连续12年无中国人得奖的历史，成为中国历史首个The Pwnie Awards大奖得主。
- 2018年全球TOP100网络安全顶级专家360占据13席位。

安全情报数据 能力第一 ★★★★★
安全存储和计算 能力第一 ★★★★★
安全可视化分析 能力第一 ★★★★★
安全数据挖掘 能力第一 ★★★★★

应对网络战/APT威胁/实网攻防：“零日”漏洞治理

零日漏洞治理能力

2019年，微软公司Blue Hat大会，**360以247次漏洞致谢位列全球第一，超过其他安全厂商之和**

2018年，360共发现苹果、谷歌、微软、华为、高通等 **全球主流厂商漏洞489个，刷新世界纪录**

10 次冠军

- 领先的人工智能分析技术

519 次致谢

- 排名全球第一

20 次夺冠

- 创造多项历史记录

71 次峰会

- 受邀参加世界顶级安全技术峰会71 次
- 发表议题演讲102 个。

11833 项专利

- 目前共申请专利11833件
- 其中网络安全专利5100 件
- 海外专利申请872 件

实战能力要求 –如 护网行动

发现问题：
能力交付 v.s. 合规交付

攻防不对等：
攻击是点，防御是面
点易攻，面难防

实战检验：
检验攻防能力，迭代防御体系

专业人员
不限手段

攻击队伍

武器库　工具库　样本库

实战攻防指挥中心

指挥调度

网络拓扑　安全保障　战法分析　可视化呈现

攻防专用通道

真实目标

预警告警　分析研判　应急处置

实时监控
实时阻断
联合防御

360参与护网行动2016/2017/2018/2019

联系方式

- 联系人：陈辉
- 电话：13826184630
- 邮箱：chenhui1@360.cn

总结

谢谢