

A N T I Y I N N O V A T I O N

安天 创造

302期

2022年07月 试行

◎ 主办：安天

◎ 400-840-9234

◎ antiynews@antiy.cn

本期焦点

勒索攻击防护

“挖矿”威胁治理

攻防演练实战

党建文化与青春风采

安天资讯

防御与治理

攻防演练

挖矿治理

勒索防护



安天网络安全冬训营之乱云飞渡

《安天创造》301期是原《安天周观察》改版后的首期。本期《安天创造》为第九届安天网络安全冬训营系列文章专刊，从“2021年网络安全回顾与展望”、“安全算力”、“闭环安全运营”和“威胁分析与综合安全”四个方面分享了安天在威胁分析研究、产品研发、防御体系建设和安全运营等方面的最新进展，以及安天历届雪雕大赛和冰雕大赛作品，为读者呈现一期“文韬”与“武略”的碰撞。

《安天创造》是安天面向客户的品牌刊物，按照安天达成客户有效安全价值的企业使命，汇聚发布安天长期从事威胁对抗工作的分析报告，分享安天在与客户并肩战斗中形成的安全理念与认知理解，总结保障和服务客户的实践经验，传递以创造性思维和工程化能力为客户解决问题的安天工程师文化，展示安天团队的创造力与青春风采。

刊首语

一切从实战出发

一切服务实战需要

2016年4月19日，习近平总书记在全国网络安全和信息化工作座谈会上发表重要讲话并指出：“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。

回顾过去，对抗过程中防御方往往处于被动局面，即使建设了态势感知，有了指控平台，勒索攻击、“挖矿”威胁依然活跃，在攻防演练中依旧捉襟见肘、惜指失掌。

立足现在，网络信息技术发展的日新月异，网空威胁也在快速地变化升级，防御体系必须紧跟威胁的步伐。特别是我国目前正处在数字化进程的快车道上，大数据、云计算等科技产业正在迅速发展，疫情催化了在线办公常态化，在获得新效益的同时也带来了新问题：网空威胁的复杂度、针对性和碎片化程度越来越高。

因此，网络安全防护工作就不能用静态的、单一的或仅从合规的思路出发，而是必须采用动态的思维结合现实场景进行纵观全局的思考，进而构筑动态综合的防御体系。同时，应对新形势下的网空威胁，安全的有效性不会一劳永逸，需要不断提升实战能力，持续保持安全运营。

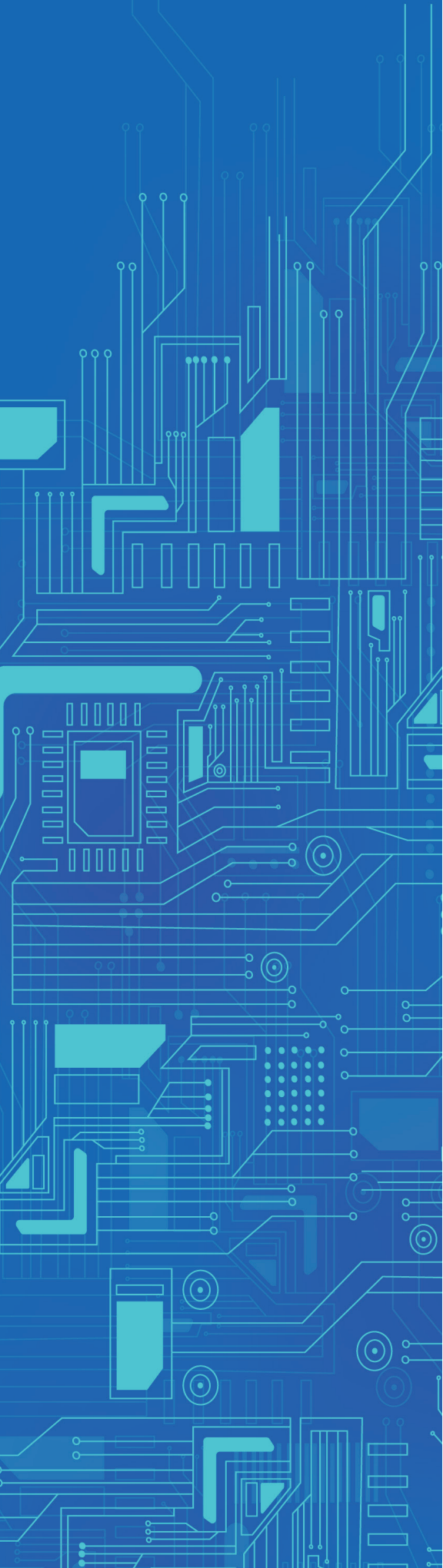
勒索攻击和“挖矿”威胁正是对安全运营能力的成果检验，攻防演练正是对体系化建设的基础校验。

知己知彼，百战不殆。2017年6月，安天提出了“有效敌情想定是网络安全工作的前提”，将“敌情想定”这一军事术语引入了网络安全领域。在后续的实践中，安天以此为基础发展出“威胁想定分

析框架”，作为重要信息系统和关键信息基础设施防护规划的基本方法。

针对勒索攻击防护，安天提出了以端点防护为主的“五层防御，两重闭环”方案：系统加固、（主机）边界防御、扫描过滤、主动防御、文档安全五个防御层次，EPP（端点防护）实时防御闭环和EDR（端点检测和响应）准实时（异步）防御闭环；针对“挖矿”威胁治理，安天提出“端点统管、持续监测、情报驱动、协同响应”的总体思路，重点对客户侧现有防护体系进行加强、完善和统管，辅以流量侧的持续监测与端点侧防护形成互补；针对攻防演练防守，安天通过综合梳理总结了“十大防守要点”，并针对性地制定了覆盖攻防演练启动、准备、决战与总结四个阶段的全生命周期解决方案，同时深入邮件安全、靶标安全、欺骗式防御等场景化进行专项防护。在实际客户服务与威胁对抗中，安天构筑的动态综合防御体系，实战安全能力的有效性，均获得了全面的验证。

着眼未来，安天正在努力以系统安全基石型产品和服务为中心，建立起依靠共性核心能力和平台化运营与威胁持续对抗的安全场景业务闭环。对于一个优秀的企业来说，不应只有依靠赛道形成的产品标准能力，而是通过合理的能力规划，以一个个产品落脚在IT场景中，与客户一同完成对数字化环境的有效治理，并服务客户实现安全能力共同运营，做到“一切从实战出发，一切服务实战需要”。



本 | 期 | 导 | 读

在网络空间安全领域，网络安全威胁风险具有极高的复杂性：一方面，网络安全形势严峻，攻击手段层出不穷；另一方面，安全事件数量不断上升，政府、教育、交通、金融、通信、能源电力等重要行业的关键信息基础设施成为攻击组织重点关注目标。在常态化的安全威胁中，勒索攻击仍然保持着广撒网与定向攻击并存，定向勒索攻击能力已达“APT”水平；“挖矿”活动在过去几年表现极为活跃，各政企机构、安全厂商以及监管部门，都共同加大了对“挖矿”威胁的防护力度；作为新形势下网络安全保障工作的重要组成部分，网络实战攻防演练成为各政企单位整体提升网空威胁对抗能力的重要活动。

面对如今网络安全威胁发展的传播方式多元、迭代变种迅猛、持久化手段丰富及产业化作业趋势等严峻形势，相关系统的安全防护策略不能仅仅立足于防范一般性、常态化风险，而是需要进行纵观全局的多维度考量，制定动态综合的系统性解决方案，甚至还要放在复杂的实战化对抗中进行检验。

本期《安天创造》聚焦实际场景防御和基础 IT 环境治理，以具有典型动态变化特征为代表的勒索防护、“挖矿”治理以及攻防演练防守三类防御场景为对象主题，综合分享实战经验与创新理念，协助客户有效构筑动态综合防御体系，提升网空威胁对抗实力。在“安天党建文化与青春风采”章节，分享了安天近期组织的系列活动和员工的青春风采。

目录
CONTENTS

PAGE

勒索攻击防护

1. 勒索攻击的四种分工角色	01
2. 勒索攻击的两种典型模式	02
3. 勒索攻击的惯用传播方式与侵入途径	03
4. “勒索攻击杀伤链”分析	06
5. 勒索攻击的四种主要勒索类型	08
6. 勒索攻击的五种重要攻击特征	10
7. 十类典型勒索家族	12
8. 勒索攻击发展趋势	18
附录：安天产品助力用户有效防护勒索攻击	22
安天部分历史公开勒索攻击相关报告简览	25

“挖矿”威胁治理

1. “挖矿”威胁治理专项方案	31
2. 智甲构建系统侧有效防护	34
3. 探海提升流量侧威胁洞见	37
案例：教育行业“挖矿”威胁治理场景价值	38
安天部分历史公开挖矿威胁相关报告简览	41

攻防演练实战

1. 防守要点与解决方案	43
2. 七大场景化专项防护	45
3. 终端 / 云主机安全防护	49
4. 流量侧持续监测	51
5. 运用文件分析提升威胁发现	53
6. 构建欺骗式防御	54
7. WEB 在线实时主动防御	58
8. 为业务系统注入“疫苗”	60
9. 快速开展应急处置与分析取证	62
附录：安天产品攻防演练价值表	63

安天党建文化与青春风采

1. 庆祝中国共产党成立 101 周年，喜迎党的二十大胜利召开	66
2. 纪念“4·19”重要讲话六周年 安天开展“总体国家安全观”宣传月活动	68
3. 逐梦新青年，我们正青春	70

安天资讯

01勒索攻击防护

安天对勒索攻击一直进行着持续的跟踪与分析：2006 年，捕获了国内最早出现的敲诈者木马 Redplus；2015 年，发布了长篇报告《揭开勒索软件的真面目》；2017 年，在“魔窟”（WannaCry）重大勒索事件响应中，率先发布全网首篇系统分析报告，快速提供了专杀免疫工具与周一开机指南，并向政企机构分发了数千张应急处置光盘，后又研发了解密工具等，获得多个主管部门好评。

针对 GandCrab、GlobelImposter、Sodinokibi 等重大流行勒索软件，安天也同样进行了应急响应与分析研判。至今，累计发布了相关分析、预警、处置建议等报告近 200 篇。

本章内容将从勒索攻击的攻击技术、行为特点、演进趋势等 8 组关键信息展开，分享如何构建有效防线。

在此，感谢安天 CERT，端点安全部奚乾悦，垂直响应部冯鑫龙、陈思等对本章内容的所做出的贡献。

勒索攻击的四种分工角色

早期的勒索攻击多半是攻击者从编写勒索病毒到投放勒索病毒一条龙完成的，但如今的勒索攻击已发展成为分工明细的产业化犯罪活动。

一次完整的勒索攻击链条里，或者说在一个勒索攻击犯罪团伙中，一般会有多种分工角色。不同攻击活动间又有很大差异，有的攻击中同一个人或同一个组织会扮演多重角色；有的攻击中分工则会更为细致。

分工确实成为勒索攻击犯罪活动的显著特点，特别是出现了 RaaS（Ransomware as a Service，勒索即服务）这种新型犯罪活动模式：通过会员、订阅或定制，向其他“攻击者”售卖勒索攻击相关服务，进一步将勒索攻击转变为“商业服务行为”。

RaaS 的出现，不仅降低了勒索攻击的准入门槛（甚至无需任何网络攻防技术与知识即可发起攻击），同时也提高了勒索攻击的防护难度，更是带来了巨大的“内鬼”作案风险。

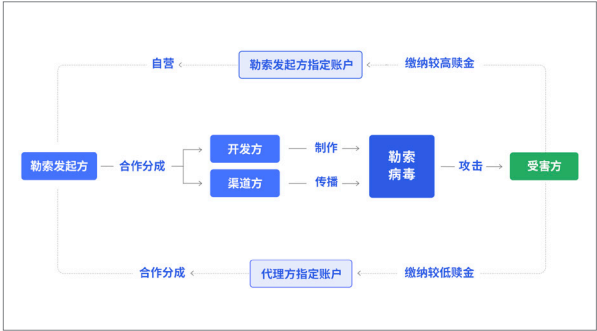


图 1 勒索攻击犯罪链条中的角色分工

1. 开发方

主要负责勒索攻击中软件、工具、生成器等相关能力的开发，是整个攻击中的上游制毒者。

在 RaaS 模式中，开发方除了负责勒索攻击的相关标品能力开发，同时也接受勒索攻击的相关定制能力开发；主要通过地下平台或“暗网”交易。

2. 发起方

是实现把勒索软件定向投放到具体攻击场景的行为角色。其有可能是一个个体，也可能是一个由组织者和执行者组成的团伙。

2.1 组织者

通过合作分成的方式，组织开发方开发勒索软件或 RaaS 平台；联合渠道商传播勒索软件；串联代理商与受害者取得联系、牟得赎金等。

2.2 执行者

勒索攻击实施阶段的重要节点事务执行，主要包括：系统入侵、病毒部署、窃密加密、勒索赎金等。

3. 渠道方

主要负责勒索软件的传播，一般由拥有诸多恶意软件传播资源的攻击组织合作参与，比较有代表性的就是僵尸网络（Botnet）。

渠道方通过利用僵尸网络控制的系统主机对勒索软件进行传播（主要有垃圾邮件与钓鱼邮件、漏洞利用、恶意网站脚本、伪装软件等），其特点是传播范围广、隐蔽性高、感染速度快，是目前勒索软件的主要传播方式之一。

注：除了传播勒索软件，僵尸网络还可以利用与勒索攻击合作发动分布式拒绝服务攻击（DDoS）、远程桌面协议（RDP）暴力破解等威胁攻击。

4. 代理方

主要负责拓展和提高勒索赎金缴纳的成功率；与勒索发起方同样是合作分成收益关系，还有的本身就是和攻击者沆瀣一气的团伙成员。代理方一般会通过网络关键词、多媒体、信息流等广告宣传，声称自己能够解密各类勒索攻击加密的文件。但实际上还存在多种情况：

有的是利用受害者不知道如何使用虚拟货币交易，赚取手续费；有的则是利用相关事件，诈骗受害者。

此前我国公安部门就曾打击掉一家以数据恢复为名义，实际上是和勒索攻击团伙勾结的所谓“数据恢复公司”。

注：值得警惕的新角色“内鬼”

当前政企机构要警惕的是：在 RaaS 全面降低了勒索攻击门槛后，“内鬼”对自身所在单位进行勒索攻击的风险会提升，需要增加预防。

5. 总结与建议

勒索攻击产业化、链条化后，勒索犯罪团伙时刻都在与安全工作者们隔空对抗，试图找到更多绕过安全机

制的办法。这也是防护能力需要持续升级改善的根本原因。安全有效性从不会一劳永逸，而需要持续有效运营。

勒索攻击的分工链条化，增加了攻击的威胁力和隐蔽性。从政企机构的资产安全角度看，构建有效防御体系才能更好应对日趋复杂的勒索威胁，防患于未然；从社会治理角度看，推动有效治理僵尸、木马、蠕虫病毒，削弱勒索攻击的传播分发能力，对勒索攻击活动进行持续跟踪分析溯源，形成国际协同的司法打击能力，都是工作抓手。

特别是要倡导在遭遇勒索攻击后坚决不交赎金的理念，面对犯罪活动不妥协，就是对正义的支持。

勒索攻击的两种典型模式

部分用户对于遭遇勒索攻击的风险往往可能存有两种误解，有些用户认为，自身资产价值不高，勒索攻击不会找上自己；也有的用户认为，非定向勒索攻击是一种比较低级的风险，不会突破自己的防护。为了澄清这些误解，本篇将重点分析勒索攻击的两种模式：非定向勒索攻击与定向勒索攻击。

安天在《2020 年网络安全威胁年报》^[1] 中曾提出：勒索软件制作者开始关注攻击成本和攻击效率；勒索攻击方式，从最初的广撒网寻找目标，逐渐地演变成对有价值的目标进行定向攻击。

因势利导，形成了当前勒索攻击在发展方向上的两级分化：

既有传统单线作业模式：非定向大规模传播 → 加密数据 → 收取赎金 → 解密数据。

也有新型链条作业模式：定向攻击 → 数据窃取 → 加密数据 → 收取赎金 / 不交赎金 → 解密数据 / 曝光数据。



图 1 非定向与定向勒索攻击图示

从目标导向理解即为：

1. 非定向勒索攻击：不求目标赎金高，但求目标数量多；
2. 定向勒索攻击：不求目标数量多，只求目标赎金高。

1. 关于非定向勒索攻击

早期非定向攻击者会采用传统的扩散蠕虫或钓鱼投放等方式，进行发散式地传播勒索软件，且不会预先对目标进行侦察、评估与筛选，对于攻击的收益也不会有

精确预估。而当前，非定向勒索攻击者大多会选用 RaaS（勒索即服务）平台或僵尸网络渠道，采取“广撒网”的方式传播勒索软件，威胁攻击对象主要为中小企业与政府机构单位。

同时，由于 RaaS 模式降低了攻击者的准入门槛，因此也助推了相关攻击参与人数的提升。

需要明确的是，部分用户对非定向勒索攻击存有误解，认为其威胁能力并不高，而事实上，非定向勒索攻击仅是一般情况下没有达到与定向攻击相较的威胁攻击水平而已，其实际的破坏力仍不容小觑。

无论是近些年较为活跃的 RaaS 平台服务提供家族 DopplePaymer、Egregor、Netwalker、REvil/Sodinokibi、DarkSide、Ryuk，还是新兴出现的 BlackMatter 等，都具有较高的威胁攻击水平。

注：提供 RaaS 服务只是勒索攻击家族为了提高非法收益，通过“价值多向变现”而拓展的商业模式，并不意味着其只提供 RaaS 服务，其同样会自主发动非定向或定向勒索攻击。

凭借传播覆盖面积足够广、攻击频次足够多、攻击参与人数足够多等“优势”，非定向勒索攻击同样是持续的勒索攻击安全防护工作的重点。

2. 关于定向勒索攻击

大部分的定向勒索攻击是由具备更高水平的攻击组织发动的，能力接近或可达到 APT (Advanced Persistent Threat，高级可持续性威胁攻击) 攻击的水平。

定向勒索攻击的特征是，事先有非常明确的攻击目标，再“有组织、有预谋、有步骤”的发动威胁攻击，以求牟取巨额收益。

定向勒索攻击与 APT 攻击高度相似，有鲜明的杀伤链化特点：

1. 预先筛选出攻击目标，由于其目的是大额甚至巨额的勒索赎金，因此，其主要瞄准的往往是中大型企业、重要政府部门 / 机构、军队单位以及关系民生的关基设施与工控系统。

2. 通过侦察手段收集、评估攻击目标的详细安全防护信息，针对性制定严密的攻击计划方案，精确计算投入成本和潜在回报（ROI）。

3. 根据攻击计划方案，充分投入部署攻击资源，如：攻击人员规模、攻击工具种类、0day 漏洞、高级恶意代码等；也包括可能获得“内鬼”的支持与配合。

基于以上信息，可以看到定向勒索攻击有超强的突防能力。

因此，用户既要做好安全的基本面，避免遭遇非定向勒索攻击；同时，对于有高价值资产的用户则需进一步提高安全防护系统和安全运营水平，防御定向勒索攻击。

3. 总结与建议

不论是非定向还是定向，只要是勒索攻击，我们都应引起足够重视。

尤其是定向勒索攻击，一些攻击者组织甚至会以跟民生相关的关键信息基础设施、工业控制系统为攻击目标；所以，建议相关用户尽快构建动态综合的勒索攻击安全防护体系。

参 考 资 料

[1] 《2020 网络安全威胁年报》.2021/01/07
https://www.antiy.cn/research/notice&report/research_report/2020_AnnualReport.html

勒索攻击惯用传播方式与侵入途径

可能部分用户还没有认识到，在如今网络环境中的每一步应用场景，几乎都有可能被攻击者利用，以实现勒索攻击的传播和侵入。

本篇基于安天历史勒索攻击分析报告及相关资料，将目前已知的攻击者惯用传播方式与侵入途径进行了归类整理，旨在为用户制定勒索攻击防护方案时提供参考。

1. 邮件传播侵入

一般为垃圾邮件、钓鱼邮件与鱼叉式钓鱼邮件，具体手段是通过邮件中的时事热点信息或与受害者相关的内容（包括标题），诱使用户打开或运行内嵌了勒索软件的附件（格式多为 Word 文档、Excel 表格、JavaScript 脚本或 exe 文件等），或点击邮件中的恶意链接。用户一旦进行相关操作，勒索软件将会自动下载和运行。

垃圾邮件在非定向勒索攻击中较为常见，以“广撒网”的方式进行传播，邮件内容一般为时事热点、广告、促销信息或伪装成打招呼邮件（如标题为“好久不见”等）。

钓鱼邮件与鱼叉式钓鱼邮件则常用于定向勒索攻击中，由于攻击者通常在事前已通过侦察手段获取到了受害者的相关信息，因此会将邮件包装成官方或工作伙伴发送的邮件（如：“XX 最新政策信息”、“XX 年度 XX 工作表”、“公司将升级 XX 系统”等相关标题与内容），甚至会模仿熟人发信的语气，增加收件人上当的概率。

这类传播及侵入的目标多为企业、高校、医院机构等单位，这些单位组织中的本地设备通常保存有较重要的文件，一旦侵入成功，即可造成极大威胁。

例：安天曾在《LooCipher 勒索软件分析报告》^[1]中指出：LooCipher 勒索软件主要通过垃圾邮件进行传播，邮件附件为包含恶意宏代码的 Word 文档。该文档诱使用户启用宏以查看文档内容，宏代码的功能为连接 Tor

服务器并下载执行程序，将该文件重命名为 LooCipher.exe，然后执行该文件。

2. 系统或软件漏洞

攻击者利用各类系统或软件漏洞（包括已公开且已发布补丁的漏洞）组合，或通过黑色产业链中的漏洞利用套件（如：Exploit Kit）来传播勒索软件。

由于未能及时修补漏洞，因此用户即便没有不安全的用网行为，也可能遭到攻击者侵入；同时，攻击者还会扫描同一网络中存在漏洞的其他设备，以扩大威胁攻击范围。

例：“魔窟”（WannaCry）就是通过“永恒之蓝”工具，利用 Windows 系统的 SMB 漏洞进行全球范围传播的。

3. 弱口令暴力破解（远程桌面控制）

由于部分服务器会使用弱口令（可简单理解为账号密码安全性较低）远程登录，攻击者便利用这一弱点实施暴力破解，实现远程登陆并手动下载运行勒索软件。例如：通过弱口令尝试暴力破解 RDP 端口、SSH 端口和数据库端口等。

即使服务器安装了安全软件，攻击者也可手动将其退出。该手段具有较高的隐蔽性、机动性，因此极难被安全软件发现。

例：2021 年 3 月，安天就曾发布《对 HelpYou 勒索软件的分析报告》^[2]，发现该勒索软除了通过邮件之外，还可以利用 RDP 弱口令渗透进行传播。

4. 僵尸网络

僵尸网络是指：采用一种或多种传播方式，将大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和

被感染主机之间所形成的一个可一对多控制的网络。

例：攻击者利用已经被僵尸网络控制的系统主机进行病毒传播，特点是传播范围广，隐秘性高，感染速度快。2021 年 8 月，安天发布了《对 AstraLocker 勒索软件的分析报告》^[3]，该勒索软件主要通过垃圾邮件和僵尸网络进行传播。

5. 恶意广告链接（网页挂马）

攻击者会向网页代理投放广告（弹窗广告、悬浮窗广告等），并在其中植入跳转链接，从而避开针对广告系统的安全机制，诱导用户点击广告、访问网站并触发恶意代码，进而下载勒索软件并执行。

有些攻击者则会选择直接攻击网站，并植入恶意代码，用户一旦访问就会感染。

也有一些攻击者会自主搭建包含恶意代码的网站，或者仿造制作与知名站点相似的“假网站”，以此来诱骗用户访问。

例：安天在《对 Maze 勒索软件的分析》^[4]中发现，该勒索软件擅长使用 FalloutEK 漏洞利用工具，或通过网页挂马的方式传播；被挂马的网页，多用于黄赌毒以及某些软件内嵌的广告页面等。

6. 软件供应链（信任转嫁）

软件供应链攻击是指利用软件供应商与最终用户之间的信任关系，在合法软件正常传播、安装和升级过程中，通过软件供应商的各种疏忽或漏洞，对合法软件进行劫持或篡改，从而绕过传统安全产品检查达到传播侵入的攻击类型。

例：2021 年 7 月 3 日，美国技术管理软件供应商 Kaseya 遭遇 REvil 勒索软件的攻击。REvil 团伙在 Kaseya 供应链攻击中利用了 0day 漏洞。据媒体报道，至少有 1000 家企业受到了攻击的影响，受害者来自至少 17 个国家，包括英国、南非、加拿大、阿根廷、墨西哥、印度尼西亚、新西兰和肯尼亚等。而 REvil 勒索团伙当时索要的赎金高达 7000 万美元^[5]。

7. 移动存储介质

攻击者通过隐藏 U 盘、移动硬盘等移动存储介质中的原有文件，创建与移动存储介质盘符、图标等相同的快捷方式并植入病毒，一旦用户点击就会运行勒索软件，或运行专门用于收集和回传设备信息的木马程序，便于未来实施针对性的勒索软件攻击行为。

由于 PE 类文件（常见后缀为 exe、dll、ocx、sys、com 的都是 PE 文件）被感染后具有了感染其他文件的能力，如果此文件被用户携带（U 盘、移动硬盘、网络上传等）到别的设备上运行，就会使得其他设备的文件也被全部感染。许多内网隔离环境，就是被藏在移动存储介质里的恶意软件感染的。

例：2021 年 3 月，安天捕获到的 BleachGap 勒索软件就具备添加自启动、改写 MBR、通过可移动介质传播等多项特征^[6]。

8. 水坑攻击

攻击者在受害者必经之路设置了一个“水坑（陷阱）”，致使受害者上当。例如：攻击者会分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，先将此网站“攻破”并植入攻击代码，一旦攻击目标访问该网站就会“中招”。

例：勒索软件“Bad Rabbit”就曾采用水坑攻击的方式传播，通过伪装成 Adobe flashplayer 欺骗用户安装，感染后会在局域网内扩散^[7]。

9. 总结与建议

勒索攻击的传播方式与侵入途径与常见的计算机网络威胁攻击大体一致，但“魔鬼藏在细节中”，用户的不当用网习惯、对系统或软件漏洞修补的忽略、对安全防护措施的忽视等，都有可能导致勒索攻击趁虚而入。

因此，养成日常安全用网习惯、构建安全防护体系、提升安全运营水平，是有效防御勒索攻击传播侵入的首要行动条件。

参考资料

[1] 《LooCipher 勒索软件分析报告》.2019/07/08
https://www.antiy.cn/research/notice&report/frontier_tech/2019190.html

[2] 《安天周观察 269 期》.2021/03/15
https://www.antiy.cn/research/notice&report/frontier_tech/2021269.html

[3] 《安天周观察 293 期》.2021/08/27
https://www.antiy.cn/research/notice&report/frontier_tech/2021293.html

[4] 《Maze 勒索病毒变种分析报告》.2019/06/10
https://www.antiy.cn/research/notice&report/frontier_tech/2019187.html

[5] REvilUsed 0-Day in Kaseya Ransomware Attack,Demands \$70 MillionRansom. 2021/07/04
https://thehackernews.com/2021/07/revil-used-0-day-in-kaseya-ransomware.html

[6] 《通过 U 盘传播的多功能勒索软件分析》.2021/03/12
https://www.antiy.cn/research/notice&report/research_report/20210316.html

[7] 《坏兔子来袭，安天智甲有效防护》.2017/10/26
https://www.antiy.cn/research/notice&report/research_report/20171026.html

“勒索攻击杀伤链”分析

勒索攻击的手段不断地在变化，攻击水平也在不断地提升，但攻击流程的共性总是存在的。理解攻击流程中各节点的价值在于，可以对其中的相关节点进行层层阻断，帮助用户建立更加安全缜密的防护体系。

本篇内容将从定向勒索攻击切入，结合“网络杀伤链”模型，分析总结出勒索攻击的重要流程节点与相互逻辑关系，尽可能通过简单易懂的方式介绍“勒索攻击杀伤链”，以使用户明确各阶段防护重点。

注：“网络杀伤链”的概念源自军事领域，它是一个描述攻击环节模型，网空威胁可划分为 7 个阶段，分别是“侦察 - 武器构建 - 载荷投送 - 漏洞利用 - 安装植入 - 通信控制 - 达成目标”。该理论也可以用来反制此类攻击，即“反杀伤链”，分别是“发现 - 定位 - 跟踪 - 瞄准 - 打击 - 达成目标”六个环节。

1. 侦察

攻击者首先会收集信息以确定被攻击目标，并侦察被攻击目标系统的防护薄弱环节。

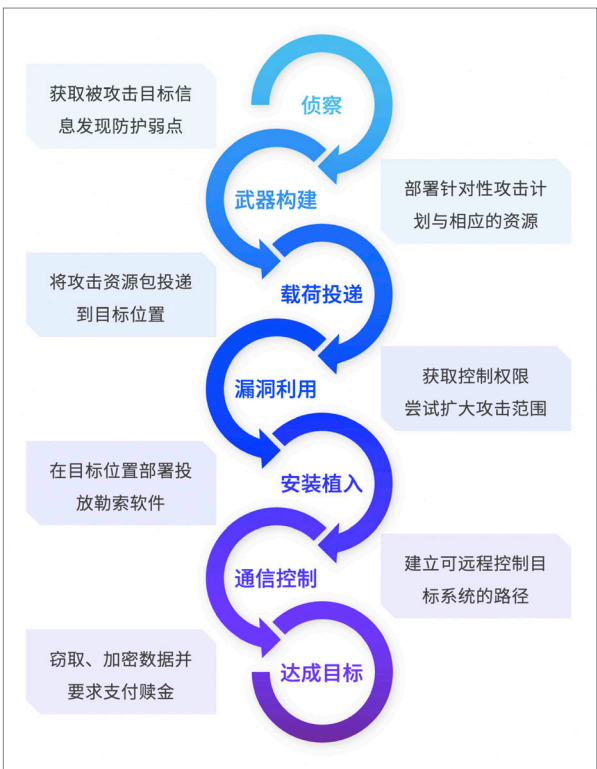


图 1 勒索攻击杀伤链示意图

1.1 收集基础信息：以定向勒索攻击为主的威胁发动前，攻击者会通过主动扫描、网络钓鱼以及在“暗网”黑市购买等方式，收集被攻击目标的网络信息、身份信息、主机信息、组织信息等，如：电子邮件地址、连接互联网的服务器等，以丰富制定攻击计划所需要的信息储备。

1.2 发现攻击入口：攻击者通过漏洞扫描、网络嗅探等方式，发现目标网络和系统存在的安全隐患，找到网络攻击的突破口。

2. 武器构建

攻击准备阶段，攻击者可能会根据发现的漏洞开发具有针对性的攻击“武器”，或者通过合作的方式从其他渠道获取成熟的攻击“武器”；之后，攻击者会利用在侦察阶段获取到的被攻击目标网络、漏洞、主机、身份和组织等画像信息，尝试制定攻击计划，并基于计划部署参与人员、开发攻击工具、确认技术细节等攻击资源。

3. 载荷投送

当准备工作结束，攻击者并不能马上发动勒索攻击，而是需要通过网络邮件、远程桌面（RDP）弱口令暴力破解、僵尸网络、网页挂马、软件供应链、移动存储介质、水坑攻击等传播方式与侵入途径，将攻击“武器”投递到目标位置。

4. 漏洞利用

这一阶段，攻击者除了需要获取更高级别的控制权限，以扩大攻击范围之外，还会想尽办法绕开或关闭安全软件，保障勒索攻击实施的效率与效果。

4.1 获取控制权限：攻击者获取到目标网络和系统的控制权限后，会进一步通过修改域策略设置等方式提升自身权限。

4.2 扩大攻击范围：攻击者还会再继续寻找系统内部漏洞，通过内网横向渗透，尽可能增加受控设备数量，扩大攻击范围；此外，攻击者还会利用权限执行修改注册表、混淆文件信息、手动退出安全防护软件等操作，以保障勒索软件的安装植入效率与运行效果。

5. 安装植入勒索软件

确保攻击范围、环境与设备可控后，攻击者会通过脚本、手动植入等手段，部署投放勒索软件，伺机手动启动或待受害者将其触发启动。

6. 通信控制

攻击者通过建立远程控制目标系统的路径，以保障对受害者实施窃密、加密等行为的全程可控。

7. 目标达成

在这一阶段，攻击者会先将被攻击目标的数据进行窃取，并在对数据完成加密后，留下勒索信息，要求受害者支付赎金。

7.1 窃取数据：获取受害者数据（包括文本、图片、音频、视频等应用数据，重要文件、磁盘引导记录等系统数据，以及数据库类文件），并回传数据至指定服务器（定向勒索攻击因事前已详细侦察受害者，会专注窃取敏感、重要及涉密部分数据）。

7.2 加密勒索：完成数据窃取后，随即加密磁盘文件，随后攻击者通常会以桌面壁纸或弹窗显示勒索信息，也有些攻击者会在桌面留下包含勒索信息的 .txt 文档；一般内容包括：勒索攻击的情况、攻击者联系方式（如“暗网”联系方式、电子邮箱等）、赎金支付地址、赎金额度、支付时限、要求受害者尽快支付赎金的威胁施压信息（如：不支付赎金就会曝光数据）等。

注：也有受害者每操作一次设备（哪怕正常点击一次鼠标）就弹窗一次勒索信息的现象。

需要明确的是，在勒索攻击中，不论是定向勒索攻击还是非定向勒索攻击，攻击者的最终目的都是获得赎金，或者通过出售窃取而来的数据获利。

8. 总结与建议

通过“勒索攻击杀伤链”可以发现，应对勒索攻击的关键在于预防，建立安全用网规范、保持安全用网习惯、及时修补漏洞、构建动态综合的防护体系，才能有效的层层阻断，从根本上提升防护能力。

勒索攻击的四种主要勒索类型

早期的勒索攻击几乎都是以加密数据为主，且与勒索攻击相关的信息大多都围绕加密展开；所以，至今仍有部分用户认为勒索攻击就只是数据加密，进而以为，就算前台没有做好安全防护措施，后台只需备份好数据也没问题。而事实上，如今的勒索攻击已经在早期的“数据加密”之上，发展出了包括窃取数据、曝光数据（泄露或出售）、破坏数据等在内的更多勒索攻击类型，不仅直接提高了整个勒索攻击产业链的危害程度，也对用户的信息资产安全防护提出了新的挑战。

本篇将主要介绍目前较为主流的四种勒索攻击类型。

1. 加密类

攻击者通常会使用多种加密算法，对用户文件（包括用户主机系统内的图片、文档、音频、视频等几乎所有攻击者关注的文件）、磁盘主引导记录、卷引导记录，甚至整个磁盘本身进行加密，最终导致用户无法读写文件、访问磁盘、正常使用或启动设备。

受害者数据一旦被加密，除了极少部分数据因为加密算法逻辑错误等因素，存在解密可能性外，大部分情况下，数据恢复都只存在理论可能，实际上基本无法硬解。

主流的勒索软件家族几乎都会在攻击中执行加密操作，加密可以看作是勒索攻击的共同攻击方式之一，例如曾造成全球范围影响的“魔窟”（WannaCry）就是通过加密实施勒索，受到攻击的设备中的图片、文档、压缩包、音频、视频、可执行程序等，几乎所有类型的文件都被加密，且后缀名均被统一修改为“.WNCRY”。

另有一些攻击者会在加密基础上，以不支付赎金就发动分布式拒绝服务攻击（DDoS 攻击）作为威胁，进一步向受害者实施勒索。

注：DDoS 攻击能使很多的计算机在同一时间遭受攻击，不仅会造成设备无法正常使用，同时造成的经济损失也非常巨大。

2. 窃密 + 泄密类

此类攻击与加密类攻击的不同点在于，攻击者会在加密之前，先窃取受害者的数据资料，在确保其窃取的数据完全回传至指定服务器后，再对数据及受害者设备实施加密。

攻击者除了勒索解密外，还会以公开、泄露、出售重要数据等为由进行多重威胁施压，持续逼迫受害者支付赎金；若受害者不支付赎金，攻击者甚至会继续威胁攻击数据中涉及到的相关人员或组织。

受害者即使事前已经对数据进行了备份而不受加密威胁，也会遭受攻击者“曝光数据”和“攻击相关人”的威胁。

注：此类多见于定向勒索攻击，详见本系列第二篇《勒索攻击的两种典型模式》。

例如，2021 年 3 月 20 日，知名电脑制造商宏碁遭遇 REvil 勒索攻击，攻击者索要 5000 万美元赎金（约 3.3 亿人民币），否则就公开被窃取和加密的数据；这些数据包括了宏碁公司的数据库数据、客户记录等等。10 月，宏碁公司再次遭遇 REvil 的攻击，其印度分公司的售后服务系统遭到破坏，超 60GB 的文件与数据被窃取。这次，攻击者仍然以泄密为条件，要挟宏碁公司支付赎金，但金额没有披露^[1]。

3. 锁定类

锁定类的攻击会全屏锁定受害者设备的屏幕，并显示包含勒索信息的图像、文字，或伪装成系统出现蓝屏错误，直接导致受害者无法登录或使用设备（系统组件同时会被禁用），进而勒索受害者支付赎金。万幸的是，此类型勒索攻击一般不会加密用户数据，具备一定的恢复可能。

此外，锁定类勒索攻击还存在于移动端。2017 年，安天移动安全团队曾对冒充为“抢红包神器”的勒索软

件进行过跟踪与分析^[2]，此类勒索软件通过强制锁屏受害者手机实施勒索，具体表现为手机一旦启动开机就立即置顶勒索界面，并提示受害者支付赎金以解锁手机，同时“禁用”手机正常按键功能，且只能输入“解锁密码”（一串数字），进而造成受害者无法正常使用手机。

4. 破坏类

破坏类勒索攻击不会对文件执行加密操作，而是采用随机字符覆写文件，永久性地破坏用户数据。在破坏数据之后，攻击者仍然会索要赎金。

安天曾发现过一个采用 .NET 框架开发的名为 Combo13 的勒索软件^[3]。该勒索软件变种最早于 2021 年 4 月被发现，主要通过垃圾邮件进行传播。Combo13 并未采用加密算法进行文件加密，而是采用随机字节数据覆盖的方式破坏文件全部原始数据，从而造成文件数据的彻底损坏。无论受害者是否支付赎金，攻击者都无法为受害者恢复文件。

此外，这类攻击还会对关键信息基础设施及工控系统造成破坏，例如，通过破坏系统文件进而导致设备无法使用。

需要重点指出的是，为了达到勒索效果最大化的目的，目前已有攻击者会将上述几种类型的攻击混合使用，致使勒索攻击呈现出“多重勒索模式”的发展趋势。本系列第八篇《勒索攻击发展趋势》中将有详细分析介绍。

5. 补充信息：为什么说数据被勒索软件加密后基本无解？

常用的加密方式包括：对称加密与非对称加密。

对称加密是最快速、最简单的一种加密方式，执行加密（encryption）与解密（decryption）使用的是同样的密钥（secret key）。常见的对称加密算法包括 DES、3DES、AES 等。

而非对称加密执行加密和解密，使用的则是不同的密钥：一对密钥——公钥和私钥。常见的非对称加密算法包括 RSA（RSA 是企业级应用标准，很多第三方的加密软件都使用 RSA 加密）、ECC（椭圆曲线加密算法）等。

正常情况下，除部分存在编程逻辑错误的文件可以解密或恢复以外，用非对称算法加密过的数据都难以解密还原。而现实中，攻击者往往并不局限于使用一项加密算法，譬如使用“AES+RSA”、“AES+RSA+ChaCha20”等混合加密手段无限度的增大解密难度。

以往被勒索软件加密后可恢复的方法主要有四种方式：

1. 加密数据时未释放内存中的对称加密算法密钥；
2. 未删除卷影可进行磁盘文件恢复；
3. 存放密钥的服务器被反制或泄露，密钥公开；
4. 攻击者主动放出密钥。

6. 总结与建议：不要支付赎金

用户若遭遇勒索攻击，应在第一时间与安全厂商或安全团队取得联系，在专业的指导下进行应急处理，把损失降到最低，尽量不支付赎金。**原因有二：**

一方面，安天在应急响应勒索攻击事件中，出现过受害者支付了赎金，却并没有得到解密的案例；有些攻击者甚至还会将数据出售或直接破坏，让受害者“钱货两空”加倍受损。

譬如前文提到的“魔窟”（WannaCry），其背后组织者虽然声称支付赎金即可解密，但该团伙只有收款通道，并不能对已支付赎金的目标进行识别，也就是说，他们根本就不知道谁付了钱，当然也就无从提供解密。

另一方面，面对犯罪活动时的不妥协，是对正义的支持；支付等于变相鼓励勒索。攻击者本质上是没有技术正义感和基本商业伦理的网络犯罪分子，其绝不可信，应坚决打击。

注：多国政府声明将从法律层面禁止支付勒索赎金。

2021 年 10 月，美、欧、澳、法、加、日等超过 30 个国家在反勒索攻击倡议在线会议后发表联合声明：将阻止使用加密货币支付赎金，以打击勒索软件团伙。在此之前，美国财政部外国资产控制办公室（OFAC）发布咨文，警告机构不要向勒索软件支付赎金，并声称此举存在违反政府对网络犯罪集团或国家黑客施加经济制裁的法律风险。一些美国州的立法机构谈论可能限制或禁

止向勒索软件支付赎金的法案^[4]。

参 考 资 料

[1] 《宏碁确认在印度的售后服务系统遭到勒索病毒攻击破坏》.2020/10/15

<https://www.bleepingcomputer.com/news/security/acer-confirms-breach-of-after-sales-service-systems-in-india/>

[2] 安天移动安全《你可能下了个假的抢红包神器》.2017/03/16

<http://blog.avlsec.com/2017/03/4544/fake-red-packets/>

[3] 《破坏而非加密文件的勒索软件 Combo13 分析》.2021/05/17

https://www.antiy.cn/research/notice&report/research_report/20210517.html

[4] 《禁止支付勒索赎金：打击勒索攻击的可行之路？》.2021/11/04

<https://www.secrss.com/articles/35743>

勒索攻击的五种重要攻击特征

目前,几乎所有的网络攻击都可以结合“网络杀伤链”模型来进行分析,但具体到不同的威胁攻击类型,其在实际操作上又有明显的区别与特点。勒索攻击从诞生以来发展至今,在一些攻击手段与攻击模式上,同样也有其显著的地方。

本篇将围绕勒索攻击目前主要的攻击特征进行分析总结。

1. 远程桌面协议（RDP）弱口令暴力破解为主要侵入手段

“弱口令”可以简单理解为：系统账户密码复杂度较低。

远程桌面协议（RDP）弱口令暴力破解成功后,攻击者可以远程登录包括普通计算机与服务器等终端进行操作。

一些用户在使用或管理终端时,为了方便记忆,经常会对系统账户使用一些简单、相似甚至统一的密码,而远程桌面协议（RDP）只需主机的账户与密码,即可访问主机内资源。弱口令虽然在一定场景下给用户带来便利,但也同时给勒索攻击者创造了可趁之机。

攻击者通过自己编写或购买的方式获得 RDP 暴力破

解工具;在取得管理员权限后,攻击者会进一步使用凭据获取工具,获得本机或域内凭据,用于内网渗透,并使用内网扫描工具,寻找网络内高价值服务器;同时,攻击者还会使用相关工具试图关闭或破坏安全防护软件。

2. 漏洞利用明显增加

随着网络安全教育普及,不少用户的警惕性都有所提升,垃圾邮件、钓鱼邮件、恶意广告等传播方式与侵入途径的成功率也因此有所降低。因此,攻击者逐步开始更多的选择利用操作系统、Web 服务、数据库、软件等关键位置存在的漏洞进行攻击侵入。

漏洞攻击往往令用户不易察觉,譬如:0day 就是一种一经发现就立即被恶意利用的安全漏洞;非常有代表性的案例是 2017 年“魔窟”(WannaCry)利用 Windows 系统基于 445 端口的 SMB 漏洞 MS17-010,造成了全球范围内的大爆发^[1]。

3. 内网横向渗透扩大攻击范围

攻击者侵入被攻击目标系统后,并不会急于立即实施窃密、加密、锁定、破坏等操作,而是继续使用弱口

令暴力破解,或利用其他漏洞进行内网横向渗透,尽可能增加受控设备数量,扩大攻击范围。

即使用户可以通过内外网隔离,来提高勒索攻击的门槛,但若前置设备或关联设备有可利用的漏洞,攻击者依然可以侵入到内网。

因为大部分勒索攻击的目的就是赎金,所以无论是非定向勒索攻击还是定向勒索攻击,攻击者都企图在受害者身上,牟取更多的赎金,而扩大勒索设备数量与数据体量,是成本较低又能直接加倍施压受害者,进而要求更多赎金的有效方式。所以,内网横向渗透扩大攻击范围,不仅是勒索攻击的典型特征,也是目前勒索攻击的必要执行流程。

4. 定向勒索攻击愈趋增多

早期勒索攻击大规模爆发时,主要通过垃圾邮件、钓鱼邮件、网页挂马等方式传播,导致大量用户深受其害。但随后攻击者发现,普通用户的数据价值相对更低,一般无法获得高额赎金;相反企业用户的资料数据一旦丢失,将会极大地影响业务的正常运转,因此企业用户往往会更积极的支付赎金来挽回数据。

所以,攻击者愈发趋向于针对企业用户或特定目标,专门实施定制化的定向勒索攻击,以求牟取更多的非法经济利益。

注:在本系列第二篇《勒索攻击的两种典型模式》中,有关于定向勒索攻击的详细分析。

5. 针对关键信息基础设施与工控系统的攻击显现

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等,是保障社会高效运转的重要组成。

工业企业网络环境主要由工业控制网络和企业信息网络组成,其中企业信息网络连接了互联网环境,形成了暴露面,即有了遭受互联网环境中勒索攻击的风险。

攻击者可以通过企业信息网络侵入或摆渡方式将勒索软件传播到工控网络中,进而导致工业控制系统无法运行。

例如,2021 年 5 月,安天 CERT 发现一起入侵工控系统并最终投放勒索软件的攻击事件,此次事件影响了欧洲一些国家的工业企业,部分用于工控业务的服务器被加密,导致工控业务系统临时关闭。经过分析,该起攻击事件归属于一个新的勒索软件家族 Cring (也被称为 Crypt3r, Vjiszy1lo, Ghost, Phantom)^[2]。

6. 总结与建议

通过勒索攻击目前的攻击特征分析不难发现,在经过长时间的发展后,攻击者不仅总结出了更有效率的攻击方式,同时也在不断的尝试造成更大破坏,进而牟取更多非法利益。

用户在短时间内无法实现安全用网规范与完善防护系统的情况下,可以针对勒索攻击的特征采取一些简单的防护措施,譬如:为系统账户设置强密码,不同账户间设置差异的且无任何关联的强密码,提高远程桌面(RDP)弱口令暴力破解的门槛;保持系统更新、应用软件更新以及安全软件更新,及时安装安全漏洞补丁,降低漏洞利用的可能等等。但这只是退而求其次的方案,面对日益复杂多变的勒索攻击态势,特别是一些网络犯罪组织所发动的定向勒索攻击,具有 APT (高级可持续威胁攻击)定向攻击水准,用户需要构建更为动态综合的勒索攻击安全防护系统与不断提升安全运营水平,才能更有效的保障自身利益免受侵害。

参 考 资 料

[1] 安天针对勒索蠕虫“魔窟”(WannaCry)的深度分析报告

<https://www.antiy.com/response/wannacry.html>

[2] 《针对工控的勒索软件 Cring 样本分析》.2021/5/28

https://www.antiy.cn/research/notice&report/research_report/20210528.html

十类典型勒索家族

本篇是在安天发布的近 50 余篇勒索攻击相关分析、预警、处置建议报告中，选取了十类典型勒索软件家族进行介绍，内容主要包括该勒索软件家族的基本概况、攻击案例与最新情况；同时，为了方便用户加深理解与记忆，每类勒索软件家族均附有其关键信息的“概览卡片”。

注：安天 CERT 均对这些勒索软件家族进行了长期的跟踪与分析，部分曾在第一时间发布过分析报告（详见文末参考资料）。

经过整理，以下勒索软件家族按首次出现时间顺序排序：

1. Petya / NotPetya^[1]

2017 年 Petya 大规模爆发，其表现与“魔窟”（WannaCry）很类似，但破坏性更大，全球多国都有遭受 Petya 攻击的案例。后来根据安全技术人员调查，Petya 也是通过“永恒之蓝”工具，利用 Windows 系统的 SMB 漏洞进行全球范围传播的。

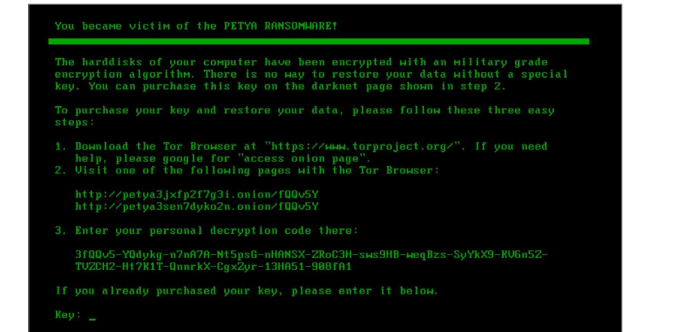


图 1-1 Petya 勒索界面信息

不久之后，NotPetya 现身。虽然它源于 Petya，但从攻击方式到破坏力，都有了非常大的提升。它利用了一个能够远程控制其他系统的工具 PsExec 进行传播。NotPetya 可以在其他电脑上远程执行恶意代码进行感染，如果一台受感染计算机拥有网络的管理员权限，那

么这个网络中的所有电脑都会被感染。

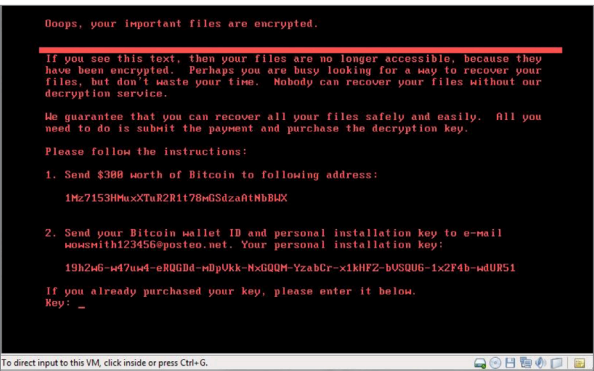


图 1-2 NotPetya 勒索界面信息

更重要的是，NotPetya 不仅可以攻击一些老旧的操作系统漏洞，就连打了补丁的 Windows 10 系统也可以进行传播，威胁指数急剧上升。

概览卡片	
出现时间	Petya 2017 年 3 月；NotPetya 2017 年 6 月
目标系统	Windows
目标群体	大中型企业
勒索金额	数额不等
传播方式	系统漏洞、远程操控
能否解密	尚未发现解密工具

2. “魔窟”（WannaCry）^[2]

2017 年 5 月，WannaCry 在全球大规模爆发，其制造者利用“永恒之蓝”工具进行传播，通过恶意代码打开微软基于 445 端口，进而传播扩散的 SMB 漏洞 MS17-010，实现远程代码执行。

据了解，“永恒之蓝”原本是美国国家安全局（NSA）“武器库”中的工具，它利用 Windows 系统的 SMB 漏洞可以获取系统最高权限，但却因不慎被泄漏成为了不法分子利用的武器。

后来据统计，此次事件至少造成了全球 150 多个国



图 2 “魔窟”（WannaCry）勒索界面信息

家约 30 万台设备受到感染，爆发后仅 3 天内就造成了高达 80 亿美元的经济损失。

注：在“魔窟”（WannaCry）重大勒索攻击响应过程中，安天率先发布全网首篇长篇分析报告《安天紧急应对新型“蠕虫”式勒索软件“Wannacry”全球爆发》^[3]，快速提供了专杀免疫工具，提供了周一开机指南，向政企机构分发了数千张应急响应处置光盘，后又研发了基于内存密钥获取的解密工具等，获得多个主管部门好评^[2]。

概览卡片	
出现时间	2017 年 5 月
目标系统	Windows
目标群体	无差别攻击
勒索金额	300 比特币
传播方式	系统漏洞
能否解密	1.0 版本可解，后续版本尚未发现解密工具

3. Globelmposter^[4]

Globelmposter 首次出现于 2017 年，通过垃圾邮件、远程桌面协议（RDP）暴力破解（以下简称“RDP 暴力破解”）和恶意软件等方式进行传播。为了提高加密速度，Globelmposter 使用了对称加密算法 AES 加密文件，并使用本地生成的 RSA 公钥，将 AES 算法的密钥加密。其开发者也在黑客论坛中开启了 RaaS（勒索即服务）模式。

Globelmposter 勒索软件家族已经出现了许多变种版本，包括十二主神系列和十二生肖系列等版本^[5]。



图 3 GlobeImposter 勒索界面信息

概览卡片	
出现时间	2017 年 8 月
目标系统	Windows
目标群体	企业、医疗系统
勒索金额	数额不等
传播方式	钓鱼邮件、RDP 暴力破解、恶意软件
能否解密	尚未发现解密工具

4. GandCrab^[6]

GandCrab 于 2018 年 1 月首次被发现，短短数月便历经 3 个版本的更迭，并迅速发展成为 2018 年第三大流行勒索软件家族。此后 GandCrab 又出现了多个变种，感染范围进一步扩大。

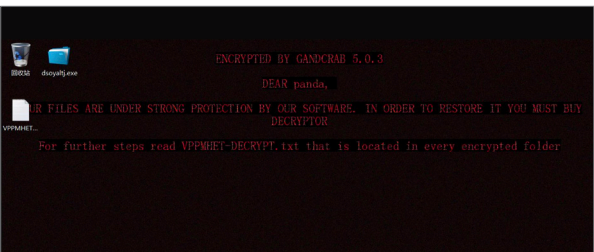


图 4 GandCrab 勒索界面信息

GandCrab 家族主要通过 RDP 暴力破解、钓鱼邮件、捆绑恶意软件、僵尸网络以及漏洞利用传播。其本身不具有蠕虫传播能力，但会通过枚举方式对网络共享资源进行加密，同时攻击者往往还会通过内网人工渗透方式，

利用口令提取、端口扫描、口令爆破等手段对其他主机进行攻击。

GandCrab 团伙曾在 2021 年 7 月短暂解散过一段时间，并公开了旧版本的解密密钥；但两个多月后，该团队部分成员卷土重来，继续制作新的变种。2021 年 11 月 4 日，一名 GandCrab 成员在科威特被捕。在此之前，曾有 GandCrab 的 RaaS 会员在韩国被捕^[7]。

概览卡片	
出现时间	2018 年 1 月
目标系统	Windows
目标群体	大中型企业
勒索金额	数额不等
传播方式	RDP 暴力破解、钓鱼邮件、捆绑恶意软件、僵尸网络、系统漏洞
能否解密	旧版本部分可解，新版本尚未发现解密工具

5. Ryuk^[8]

Ryuk 最早于 2018 年出现，是一种通过大规模垃圾邮件活动以及漏洞利用工具包进行传播的家族。Ryuk 的前身是 Hermes 勒索软件家族，它是由黑客组织 GRIM SPIDER 幕后操作运营，GRIM SPIDER 是一个网络犯罪集团，至今一直活跃。

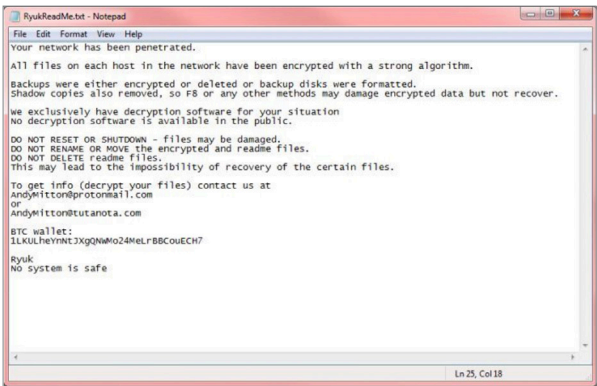


图 5 Ryuk 勒索界面信息

Ryuk 的攻击目标主要集中在大中型企业，其目的自然是索要巨额赎金。例如：2019 年 6 月 11 日，Bonfiglioli 公司遭到 Ryuk 勒索攻击，要求赎金高达 2400 万欧元；到了 2020 年，有数个大型工控企业包括

钢铁、采矿、工业建筑等行业受到 Ryuk 勒索软件攻击，导致企业部分服务器瘫痪、系统下线等严重后果^[9]。

概览卡片	
出现时间	2018 年 8 月
目标系统	Windows
目标群体	传统企业为主，尤其是大中型企业
勒索金额	几十万到上百万甚至上千万美元不等
传播方式	钓鱼邮件、系统漏洞、僵尸网络
能否解密	尚未发现解密工具

6. REvil/Sodinokibi^[10]

最早这款勒索软件被称为 Sodinokibi，后来国外有一些安全研究人员基于 Sodinokibi 的解密工具又称这款勒索软件为 REvil 勒索软件，于是这款勒索软件就有两个名字。

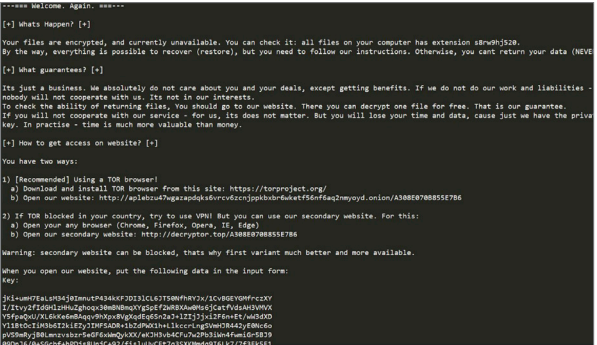


图 6 REvil/Sodinokibi 勒索界面信息

2019 年，REvil 出现时被视作 GandCrab 的继任者，因为根据一些安全专家的研究，REvil 与 GandCrab 在功能上有着许多相似之处。REvil 早期同样以邮件、伪装 Flash 插件等形式入侵，后来又新增了“多重勒索”手段。

作为勒索软件领域最臭名昭著的家族之一，REvil 的攻击目标通常是企业，尤其是大型企业，索要的金额从几百万美元到上千万美元不等。例如：2021 年 7 月 2 日，REvil 使用 Kaseya 0Day，攻击了全球 60 家托管服务提供商和 1500 多家企业。在成功加密企业数据后，REvil 要求受害者支付高达 7000 万美元的巨额赎金，以换取解密密钥，并保证不会曝光数据。

2021 年 11 月 8 日，欧洲刑警组织发布的一份声

明显示，罗马尼亚当局于 11 月 4 日逮捕了两名涉嫌与 REvil 有所关联的人士。此外，今年上半年还有另外三名 REvil 团伙嫌疑人落入法网，因此目前共有五人被缉拿归案^[11]。

概览卡片	
出现时间	2019 年 4 月
目标系统	Windows
目标群体	传统企业为主，尤其是大中型企业
勒索金额	几百万美元到上千万美元不等
传播方式	钓鱼邮件、伪装插件、RDP 暴力破解、系统漏洞
能否解密	部分早期版本可解，其余尚未发现解密工具

7. DoppelPaymer^[12]

DoppelPaymer 最早于 2019 年 6 月被发现，主要通过 RDP 暴力破解和垃圾邮件进行传播，邮件附件中带有

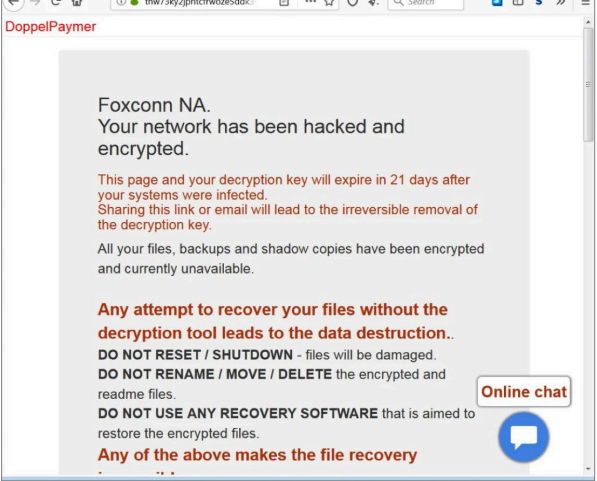


图 7 DoppelPaymer 勒索攻击富士康时的勒索界面信息

DoppelPaymer 勒索软件与 INDRIK SPIDER 组织的 BitPaymer 勒索软件在部分代码段、勒索信内容和支付赎金网页较为相似，故有专家怀疑 DoppelPaymer 勒索软件隶属于 INDRIK SPIDER 组织。

概览卡片	
出现时间	2019 年 6 月
目标系统	Windows

目标群体	大中型企业
勒索金额	数额不等
传播方式	RDP 暴力破解、垃圾邮件
能否解密	尚未发现解密工具

8. LockBit^[13]

LockBit 最早被发现于 2019 年 9 月，主要通过 RDP 暴力破解进行传播侵入，2021 年发布了 2.0 版本。攻击者通进入系统后会首先使用网络扫描器找到域控制器，得到域控制器权限后通过横向渗透释放并运行勒索软件。LockBit 采用 AES+RSA 加密算法组合的形式加密文件，目前被加密的文件暂无法解密。

LockBit 会在受感染的组织内进行自我传播，而无需



图 8 LockBit 勒索界面信息

人工定向，甚至可以做到在几个小时内影响一个公司的网络，并部署勒索软件加密数百台设备；LockBit 还可以更改系统的桌面背景、唤醒离线设备、通过联网打印机反复打印勒索信以引起受害者的注意。

同时，LockBit 组织声称提供“全世界”最快的加密和文件窃取 (StealBit) 工具，正常情况下，可以在 20 分钟内窃取 100GB 的文件，并上传到云端。

概览卡片	
出现时间	2019 年 9 月
目标系统	Windows
目标群体	企业
勒索金额	数额不等
传播方式	RDP 暴力破解为主
能否解密	尚未发现解密工具

9. Avaddon^[14]

Avaddon 首次出现在 2020 年 6 月，由来自俄罗斯的某地下黑客论坛出售，由 C++ 语言编写，采用 RSA-2048 和 AES-256 加密算法对文件进行加密。在安全研究人员于 2021 年 2 月发布了公开解密器后，Avaddon 组织者又迅速支持其合作成员进行了更新。从那时起，Avaddon 的活动激增，其开发者正在积极地为这个活跃的 RaaS（勒索即服务）平台研发下一代工具。

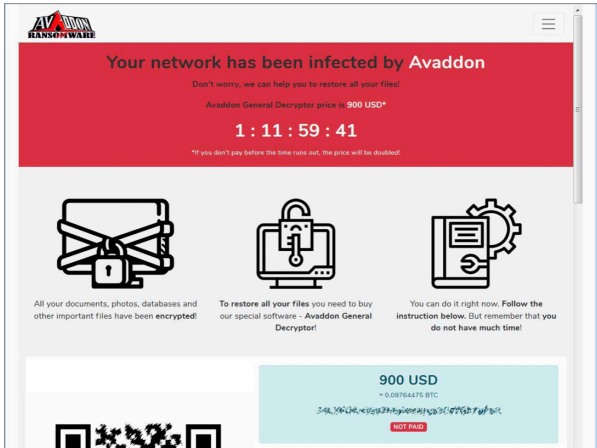


图 9 Avaddon 勒索界面信息

2021 年 5 月，保险巨头安盛位于泰国、马来西亚、中国香港、菲律宾的分公司遭受 Avaddon 勒索攻击。Avaddon 在其数据泄露网站上称，已经从安盛亚洲业务中窃取 3TB 的敏感数据，包括客户的医疗报告、身份证复印件、银行账户报表、索赔表格、付款记录、合同信息等。

Avaddon 的传播方式多种多样，前期主要通过垃圾邮件附件 JS/PowerShell 恶意脚本等无文件技术进行传播，后期则通过 Phorpiex 僵尸网络进行传播；同时安全技术人员还发现，该勒索软件通过垃圾邮件附带 Excel 4.0 宏恶意代码进行传播。

概览卡片	
出现时间	2020 年 6 月
目标系统	Windows
目标群体	大中型企业
勒索金额	数额不等
传播方式	第三方传播渠道，如 Phorpiex 僵尸网络等
能否解密	安天垂直响应平台（vs.antiy.cn）可获取解密工具

10. DarkSide^[15]

DarkSide 组织开发的勒索软件于 2020 年 8 月首次出现，具有 RaaS 模式，即除 DarkSide 自运营外，还存在其他的合作攻击者。

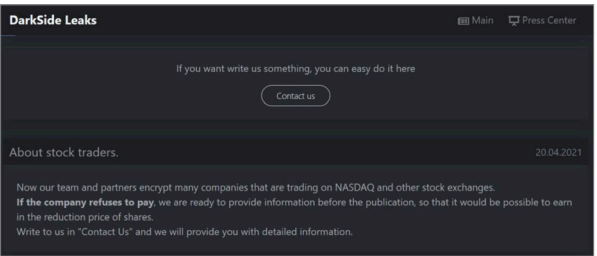


图 10 DarkSide 勒索界面信息

DarkSide 勒索软件采用多线程等技术加密，加密速度较快，加密相同文件的用时较少；此外，DarkSide 可以感染 Windows 和 Linux 系统。DarkSide 采用“窃密 + 勒索”的组合形式对受害者发起攻击，这意味着攻击者不仅会加密数据，而且还会以窃取的数据威胁受害者：如果不支付赎金就将其数据公开。

DarkSide 的组织者会在发起攻击前评估企业的财力，然后再决定勒索的金额。2020 年 8 月 10 日，该组织在其暗网论坛中声明，根据他们的“组织原则”，医疗、教育、殡葬、非营利团体及政府等机构不在他们的攻击范围内。

当地时间 2021 年 11 月 4 日，美国国务院宣布最高悬赏 1000 万美元，奖励任何“能够识别或定位在 DarkSide 勒索软件跨国有组织犯罪集团中担任关键领导职务者”的信息。原因有可能是该组织在 2021 年 5 月发动的针对美国最大成品油管道运营商 Colonial Pipeline 的攻击，该攻击导致了美国东部沿海主要城市输送油气的管道系统被迫下线。^[16]

概览卡片	
出现时间	2020 年 8 月
目标系统	Windows、Linux
目标群体	传统企业为主
勒索金额	平均 650 万美元左右
传播方式	钓鱼邮件为主
能否解密	安天垂直响应平台（vs.antiy.cn）可获取解密工具

11. 总结与建议

由于篇幅所限，主要对部分勒索软件家族情况做介绍，实际上各式各样的勒索软件及其相关变种还有很多；2021 年 7 月，美国联邦调查局 (FBI) 的官员就曾表示，该机构正在追踪的活跃勒索家族团伙就有超过 100 多个；而网络安全公司 Emsisoft 的分析师也指出，被研究人员发现的勒索家族团伙已有超过 1000 个^[17]。

同时，根据公开信息整理获悉，勒索软件的数量在 2021 年出现了显著的上升，据 SonicWall 《2021 上半年网络威胁报告》（2021 Cyber Threat ReportMid-Year Update）^[18] 称，上半年全球勒索攻击量（3.047 亿次）已经超过了 2020 年全球勒索攻击量的总合（3.046 亿次），同比增长了 151%。

数据显示，目前勒索软件的数量与勒索攻击的数量都在快速增长，即使用户在遭受勒索攻击后，可以求助安天 CERT 与安天安全服务中心通过专业的应急响应能力，尽最大可能协助挽回损失。但从风险防范角度来看，事前预防远胜于事后的亡羊补牢。尽快构筑起勒索安全防护系统，提升安全运营能力，才能有效阻止勒索攻击的发生。

注：对于安天全线产品如何支持客户构建有效防御体系，请参考本系列附录《安天产品助力用户有效防护勒索攻击》。

参 考 资 料

[1] 《安天针对攻击乌克兰等国的“必加” (PETYA) 病毒分析与应对》.2017/06/28
<https://www.antiy.com/response/petya/petya.pdf>

[2] 《安天针对勒索蠕虫“魔窟” (WannaCry) 的深度分析报告》.2017/05/13
<https://www.antiy.com/response/wannacry.html>

[3] 《安天紧急应对新型“蠕虫”式勒索软件“wannacry”全球爆发》.2017/05/13
https://mp.weixin.qq.com/s?__biz=MjM5MTA3Nzk4MQ==&mid=2650170534&idx=1&sn=dcdc3ff25c3594b49bc4e6c53c9fd123&scene=21#wechat_redirect

[4] 《警惕 GLOBEIMPOSTER 勒索软件，安天智甲有效防护》.2018/02/08

https://www.antiy.cn/research/notice&report/research_report/20180208.html

[5] 《2019 年网络安全威胁回顾与展望》.2020/01/08

https://www.antiy.cn/research/notice&report/research_report/2019_AnnualReport.html

[6] 《GandCrab 勒索软件着眼“达世币”，安天智甲有效防护》.2018/02/28

https://www.antiy.cn/research/notice&report/research_report/20180228.html

[7] 《曾发动今年最严重网络攻击的勒索软件团伙被抓了》.2021/11/09

<https://mp.weixin.qq.com/s/QDQZ6R-X5hEdSQCXE55tbw>

[8] 《Ryuk 勒索软件分析报告》.2019/01/07

https://www.antiy.cn/observe_download/observe_169.pdf

[9] 《多起攻击工业企业的勒索软件 Ryuk 分析及防御建议》.2020/03/20

https://www.antiy.cn/research/notice&report/research_report/20200320.html

[10] 《Sodinokibi/REvil 勒索组织近期活动梳理与最新样本分析》.2021/09/18

https://www.antiy.cn/research/notice&report/research_report/20210918.html

[11] 《涉嫌部署 REvil 勒索软件的网络攻击者被捕》.2021/11/09

<https://bbs.antiy.cn/forum.php?mod=viewthread&tid=96177&extra=page%3D1>

[12] 《DoppelPaymer 勒索软件变种分析报告》.2019/11/25

https://www.antiy.cn/research/notice&report/frontier_tech/2019209.html

[13] 《勒索软件 Lockbit 的攻击正在影响美国中小型企业》.2020/08/06

<https://www.bleepingcomputer.com/news/security/interpol-lockbit-ransomware-attacks-affecting-america>

[14]《勒索软件团伙正在开发第二版 Avaddon》. 2021/04/06

<https://www.sentinelone.com/labs/avaddon-raas-breaks-public-decryptor-continues-on-rampage/>

[15]《关于美燃油管道商遭勒索攻击关停事件的初步研判和建议》.2021/05/10

https://mp.weixin.qq.com/s?__biz=MjM5MTA3Nzk4MQ==&mid=2650182542&idx=1&sn=7c219a92af952c834c3eb0dbb8fce7b0&scene=21#wechat_redirect

[16]《针对美燃油管道商遭勒索攻击关停事件总结》.2021/06/09

https://mp.weixin.qq.com/s?__biz=MjM5MTA3Nzk4MQ==&mid=2650182954&idx=1&sn=881d61a5072f022bd477b57473ea5539&scene=21#wechat_redirect

[17] 光明网《美 FBI：正追踪超 100 个活跃勒索软件团伙半数或难破获》.2021/07/30

<https://m.gmw.cn/baijia/2021-07/30/1302445105.html>

[18] SonicWall《2021 上半年网络威胁报告》(2021Cyber Threat Report Mid-Year Update) .2021/08/26

<https://tdcontent.techdata.com/techsolutions/security/files/mid-year-2021-cyber-threat-report.pdf>

勒索攻击发展趋势

1. 勒索攻击已经成为全球面临的主要网空威胁之一

2021 年 6 月，一项面向全球 2600 名安全专家的调查显示，由于勒索攻击在过去 12 个月里的频繁活动，受访专家们将勒索攻击列为全球主要网空威胁之一^[1]，足以说明勒索攻击对全球网络安全的威胁程度。

如今，政企大力推动数字化转型，个人与组织对互联网、云计算等新兴技术的依赖日益增加，勒索攻击的数量与水平也在随之增加。

在此背景下出现的跨平台勒索攻击、具有 APT（高级可持续性威胁攻击）水平的定向勒索攻击、多重勒索、RaaS 等等，都是勒索攻击者新增的模式。

2. 多系统平台勒索攻击愈趋成熟

目前，勒索攻击虽然主要集中在 Windows 系统平台，但跨平台的勒索攻击也愈趋成熟。例如，REvil / Sodinokibi、DarkSide、Conti 等勒索软件家族都开发了针对 Linux 系统的勒索软件；而针对 macOS 操作系统，也出现了 MacRansom、MacSpy 等勒索软件。

尽管目前尚未爆发针对移动平台的大规模勒索攻击

事件，但由于移动用户数量众多，因此安全隐患仍不容小觑。安天移动安全团队就曾对冒充为“抢红包神器”的勒索软件进行过跟踪和分析^[2]，该软件对用户的个人隐私、财产安全造成了严重威胁。特别提醒：Android 系统和进行过“越狱”操作的 iOS 系统都有可能成为勒索攻击的对象，下载应用软件时要注意甄别，建议选择官方平台下载，不要选择非官方平台下载或使用未知来源的应用软件。

此外，EKANS^[3]、Cring^[4]等专门针对工控系统的勒索攻击开始涌现，可对工业生产造成严重破坏影响。

3. “多重勒索”模式带来更大威胁

定向勒索攻击中“多重勒索模式”的出现，再一次提升了勒索软件的威胁指数，也为安全行业带来了新的挑战。

早期勒索攻击者的手段往往是破坏数据，后来为获取更多利益，逐步演变出了窃取数据、加密数据相结合的“双重勒索”模式；如今，攻击者又在“双重勒索”的基础上，增加了新的手段，如：将窃取的数据出售、

泄露，或发动 DDoS 攻击，甚至继续勒索攻击窃密数据中涉及到的相关人员或组织，强势施压受害者支付赎金，形成“多重勒索”^[5]。

多重勒索模式的出现更打破了部分用户此前对于“灾备是‘万灵药’”的认知。一些攻击者会在攻击用户常用设备的同时，对备份数据的设备也进行攻击，导致受害者失去恢复数据的可能，并以此来提升勒索赎金的金额。本系列第七篇《十类典型勒索家族》中提到的 Ryuk 即具有同时攻击备份数据的特征^[6]。

4. 勒索软件与 APT 联系在一起发动攻击

勒索软件与 APT 联系在一起，可谓开启了一个新的威胁时代。APT 不是一种单一的攻击技术手段，而是通过成建制的团队，遵循严密的作业手册，根据目标的情况，从攻击装备库中取用恶意代码、漏洞利用程序等进行的攻击组合。主要以战略目标、基础设施和特定高价值目标为对象，具有手段高级、时效持久的一种攻击方式。

APT 和勒索软件的关系常见有两种：

4.1 攻击者发动的定向勒索攻击，攻击能力已达 APT 水平：

被攻击目标多为大型机构或组织（如中大型企业、政府部门等），攻击者会针对不同目标进行定制化攻击，以求在提高攻击成功率的同时，尽最大可能获利。在攻击者眼中，这种攻击模式是一起投入低、回报高、见效快的投资；这也符合其始终利润最大化动机与目标。

注：“投入低”的说法是相对回报而言的。实际上，APT 攻击的投入，比大部分其他类型网络攻击的投入更高。

4.2 APT 伪装成勒索攻击发动威胁攻击：

通过分析一些案例，研究人员还发现，APT 组织会将勒索软件作为探路的手段，或者逃跑的“烟雾弹”，甚至是作为攻击结束后毁灭踪迹的方法，帮助掩盖和抹去更严重攻击的证据。某些工具表面看似勒索软件，会加密数据、发布勒索通知以及索要赎金，但实际上，这些软件会悄悄删除端点上的数据，同时让防御者相信数据丢失的原因是由于勒索软件的随机攻击；还有一些工

具会抹去攻击者入侵的痕迹，例如他们使用过的工具、停留的时间、以及访问或窃取了哪些信息。

4.3 补充信息：

从“魔窟”（WannaCry）到“伪必加”（NotPetya）再到“坏兔子”（BadRabbit），勒索模式逐渐发生了变化，勒索软件不再是单纯的勒索赎金，而是表现出了一种新的准军事攻击的模式。这种新模式下的勒索软件依然披着勒索的外衣，伪装自己，试图混淆视听。

部分勒索软件其本质目的已经不是勒索赎金，而是实现对特定目标、特定区域设施的打击破坏。这种攻击模式不同于以往 APT 表现出的高度定向、指哪打哪的模式，而是基于一定的地缘条件，针对特定区域的目标投放木马，借由勒索软件自身的传播进行破坏。例如，“伪必加”是通过一款会计服务与业务管理软件的更新进行传播，它主要投放区域是乌克兰地区；“坏兔子”的投放入口是东欧的一些新闻媒体网站，许多东欧当地的政府部门和企业都受到了攻击；“Erebus”的初始投放入口是韩国网络托管公司“Nayana”；甚至还出现了“Magniber”这种只对韩文系统的计算机进行破坏的勒索软件。这种区域半定向的攻击方式迅速地给投放区域带来了负面的影响，同时由于其传播的（不）定向性，在一定程度上增加了安全研究人员的调查周期^[7]。

5. RaaS 模式愈发成熟壮大

RaaS 模式通过收取会员费用、购买勒索软件、订阅攻击服务等形式，将勒索攻击转变为“商业服务行为”。购买者甚至无需任何网络攻防技术和知识，仅通过“付费会员”身份，就能获取勒索攻击资源，进而发起攻击。

例如，安天曾监测到的商业窃密木马 Agent Tesla^[8]，该木马最早于 2014 年在其官方网站进行销售，价格根据选择的功能在几美元到几十美元之间不等。之后该木马转为在地下论坛出售，更新频繁，主要通过钓鱼邮件进行传播，邮件附件伪装成与邮件主题相关的内容，诱导受害者点击。

安天提醒：通过 RaaS 模式购买相关服务实施勒索攻击，同样是严重的网络犯罪行为。2021 上半年，媒体

曾报道过 GandCrab 的 RaaS 模式会员在韩国被捕的消息^[9]，各国政府都在对此类行为进行严厉打击。

6. 勒索软件与“挖矿”木马“狼狈为奸”

近年来，加密货币的价格水涨船高，一些不法分子为了获得更多的加密货币，选择将勒索软件与“挖矿”木马相结合发动威胁攻击，以求利益最大化。

由于勒索软件和“挖矿”木马的传播方式、侵入途径、攻击方法非常相近，攻击者会在攻击过程中将二者同时施放，受害者的设备不仅会遭受勒索攻击，还会被攻击者用来“挖矿”。

注：“挖矿”木马是攻击者通过钓鱼网站传播、捆绑传播、僵尸网络传播、弱口令暴力破解以及漏洞利用等手段，非法入侵到受害者的计算机中将其感染为“矿机”，从而利用受害者的计算机算力、网络与电力等资源计算生产虚拟货币，进而牟取经济收益的一种计算机病毒程序。

7. 针对关键信息基础设施与工控系统的攻击显现

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等，是保障社会高效运转的重要组成。

工业企业网络环境主要由工业控制网络和企业信息网络组成，其中企业信息网络连接了互联网环境，形成了暴露面，即有了遭受互联网环境中勒索攻击的风险。攻击者可以通过企业信息网络侵入或摆渡方式将勒索软件传播到工控网络中，进而导致工业控制系统无法运行。

例如，2021 年 5 月，安天 CERT 监测到一起入侵工控系统并最终投放勒索软件的攻击事件，此次事件影响了欧洲一些国家的工业企业，部分用于工控业务的服务器被加密，导致工控业务系统临时关闭。经过分析，该起攻击事件归属于一个新的勒索软件家族 Cring（也被称为 Crypt3r, Vjiszy1lo, Ghost, Phantom）。

8. 勒索软件产业链出现成熟的第三方数据泄露平台

勒索软件发展至今，一些攻击者逐渐发现：以加密数据为威胁获得的赎金，已经远不如以泄露数据相要挟而获得的赎金多。一方面是因为个人、企业或政府机构对于数据保密的重视程度逐年提升，另一方面是因为各国政府对数据泄露的惩罚越发严厉。

而从威胁程度上来看，数据加密虽然难解，但还有可能通过备份等方式进行恢复；可一旦重要数据资料遭到泄露（特别是涉密数据），对于某些受害者来说将会是毁灭性的打击，尤其是尚处在保密阶段的政策、产品、研究、人员等相关信息数据。

于是，勒索软件的组织者们也开始调整策略，从加密向泄密“转型”。例如：Babuk 组织就宣布“将不再进行数据加密勒索，全面转型数据泄露勒索”^[10]。

与此同时，“暗网”市场内提供泄露数据交易的服务平台也应运而生。除了 2019 年成立的 Dark Leak Market，2021 年新出现的 Marketo、FileLeaks 和 Lorenz 都较为活跃。其中，Marketo 在不到半年的时间里，就上架了日本富士（4GB）、德国 Puma（1GB）、法国 GigaTrib（5GB）等超过 50 家企业的被窃数据（截至 2021 年 10 月数据）。据统计，2019 年以来，勒索软件攻击组织已合计从“暗网”泄露了超过 2100 家企业被窃数据^[11]。

9. 模仿、冒充“知名”勒索软件家族进行勒索

2021 年 6 月，安天监测到一个勒索语言为中文的勒索软件，该勒索软件采用 .Net 语言编写，模仿 Locky 勒索软件，对加密的文件追加“.locky”后缀名^[12]。

同时，由于一些勒索软件是开源的，因此一定程度上诱发了其他攻击者的模仿。

还有一些具备一定攻击技术，但整体水平不高的攻击者，会在控制、锁定受害者设备后，弹出一封“知名”勒索软件家族的同款勒索信，让受害者产生“遭受了强力勒索攻击”的错觉。但实际上，这类攻击甚至可能都无法加密受害者数据。

这样的做法无疑是为了获得较高的勒索赎金，但此

类攻击者往往只敢去攻击安全防护不完善的用户。在面对勒索防御能力强、安全水平运营高、应急响应速度快的安全防护系统，这种“纸老虎”勒索攻击很快就会露馅。

要明确的是，勒索攻击是毫无技术正义感和基本商业伦理的网络违法犯罪行为，与崇高的技术追求极客精神绝无关系，任何形式的模仿、冒充甚至崇拜都应坚决打击抵制。

10. 总结与建议

通过本篇介绍勒索攻击的发展趋势可以看出，未来的勒索防御仍充满挑战且不容乐观。

结合前文内容，可总结 3 点关键信息：

1. 如今的勒索攻击已发展成为分工明细的产业化犯罪活动；
 2. 目前勒索软件的数量与勒索攻击的数量都在快速增长；
 3. 当前勒索攻击的威胁能力持续上升（已达 APT 级威胁水平）。
- 严峻的客观环境势必需要用户构建更为动态综合的勒索攻击安全防护体系，才能更有效的抵御勒索攻击威胁，保障自身利益安全。

参 考 资 料

- [1] 2021Thales Data Threat Report. 2021/06/02
<https://iwanta.tech/news/thales-publishes-its-global-data-threat-report-2021/>
- [2] 安天移动安全《你可能下了个假的抢红包神器》.2017/03/16
<http://blog.avlsec.com/2017/03/4544/fake-red-packets/>
- [3] ThreatAssessment: EKANS Ransomware. 2020/06/26
<https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/>
- [4] 《针对工控的勒索软件 Cring 样本分析》.2021/5/28
https://www.antiy.cn/research/notice&report/research_report/20210528.html

[5] 《针对美燃油管道商遭勒索攻击关停事件总结》.2021/06/09

<https://mp.weixin.qq.com/s/I4u9KzcqTQgV0ambj6txeQ>

[6] 《Ryuk 勒索软件分析报告》.2019/01/07

https://www.antiy.cn/observe_download/observe_169.pdf

[7] 《2017 网络安全威胁的回顾与展望》.2018/07/07

<http://www.antiy.com/response/20180707.html>

[8]《商业窃密木马 AgentTesla 新型变种分析》.2021/08/12

https://www.antiy.cn/research/notice&report/research_report/20210812.html

[9] 《曾发动今年最严重网络攻击的勒索软件团伙被抓了》.2021/11/09

<https://mp.weixin.qq.com/s/QDQZ6R-X5hEdSQCXE55tbw>

[10] 《Babuk 宣布退出加密勒索，将专注于数据盗窃勒索》.2021/04/30

<https://www.bleepingcomputer.com/news/security/babuk-quits-ransomware-encryption-focuses-on-data-theft-extortion/>

[11] 《安天每周安全事件 - 第 278 期安全事件》. 2021/05/10-2021/05/16

https://www.antiy.cn/research/respond/threaten_info/2021278.html

[12] 《模仿 Locky 的中文勒索软件分析》.2021/06/11

https://www.antiy.cn/research/notice&report/research_report/20210611.html

附录：安天产品助力用户有效防护勒索攻击

1. 安天智甲全面构筑端点系统侧安全防线

绝大多数勒索攻击都是以主机系统为攻击点，以主机上的数据为侵害对象。与此同时，随着加密协议正在全面削弱防火墙等安全边界，网络安全支点正在回归主机系统安全侧。面向政企侧端点场景，安天打造了智甲终端防御产品家族。智甲基于 UES（统一端点安全）理念研发，将病毒查杀、配置加固、可信环境验证、主动防御、分布式防火墙、介质管控、Web Server 防护等模块积木化组合，可以有效覆盖包括传统桌面、工作站、服务器、虚拟化、容器等场景的安全需求，对包括 Windows、Linux、Android 以及欧拉、麒麟、统信等国产操作系统都能有效建构系统内核层防御。

智甲针对勒索攻击构建了“五层防御，两重闭环”的防护解决方案。五层防御即系统加固、（主机）边界防御、扫描过滤、主动防御、文档安全五个防御层次，两重闭环是 EPP（端点防护）实时防御闭环，和 EDR（端点检测 and 响应）准实时 / 异步防御闭环。

凭借这样的机理设计，辅以每日 10 次病毒库本地升级，云端库实时升级，威胁情报定时推送，安天智甲可以有效阻止病毒落地、阻断恶意行为、保护重要文档，全面有效的保障用户免受勒索攻击威胁。

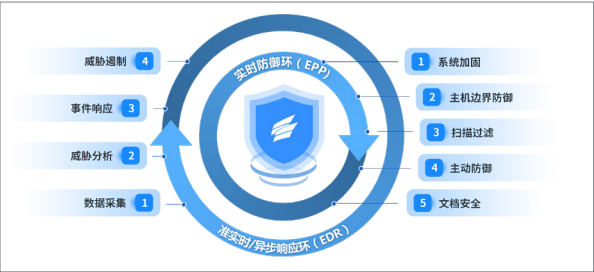


图 1 智甲终端防护系统防护勒索病毒原理示意图



图 2 智甲（桌面版）拦截勒索攻击与文档保护界面示例

安天智甲终端防御系统防护勒索病毒的机理表	
防护层级	技术原理
系统加固	通过基线和补丁检查功能，实现对系统配置脆弱点的检查修补、补丁加固和系统自身安全策略调整等，从而减少包括开放端口、弱口令、不必要的服务等勒索攻击的暴露面，削弱漏洞利用的成功率。
（主机）边界防御	通过分布式主机防火墙和介质管控功能，拦截扫描、入侵数据包，阻断攻击载荷传输，拦截 U 盘、光盘等插入自动运行，使勒索攻击难以获得主机入口。
扫描过滤	基于安天 AVL SDK 反病毒引擎对文件对象、扇区对象、内存对象、注册表数据对象等进行扫描，判断检测对象是否是已知病毒或者疑似病毒，从而实现精准判断查杀。
主动防御	基于内核驱动持续监控进程等内存对象操作行为动作，研判是否存在持久化、提权、信息窃取等攻击动作，判断是否存在批量读写、删除、移动文件或扇区等操作，并文件授信（签名验证）机制，过滤正常应用操作动作以降低误报。
文档安全	依靠部署多组诱饵文件并实时监测，诱导勒索病毒优先破坏，达成欺骗式防御效果。采用多点实时备份机制，即使正常文档被加密也可快速恢复。

2. 安天全线产品支持用户构筑全面防护体系

当前，一些网络犯罪组织所发动的定向勒索攻击，具有 APT（高级可持续威胁攻击）定向攻击水准，用户需要更为动态的综合勒索攻击安全防护体系，安天全线产品可以有效支撑构筑用户防御阵地。

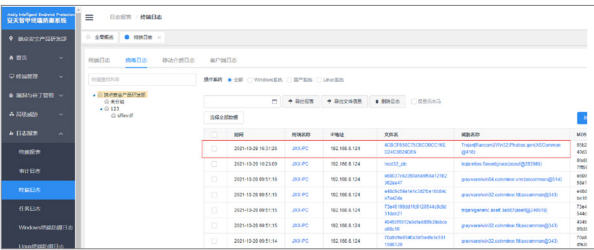


图 3 智甲管理中心威胁告警与处置界面

安天智甲终端防御系统防护勒索病毒的机理表			
产品品牌	产品定位	部署方式	在勒索攻击安全防护上的价值
智甲 终端防御系统	UES 统一端点防御 覆盖 EPP\EDR\CWPP	安装（或原厂预制） 在系统主机上。	基于主机加固机制减少攻击暴露面，基于边界防御机制拦截网络连接和介质运行，通过驱动级的监控，实时感知本地新增文件及其动作，调用安天 AVL SDK 反病毒引擎进行精准检测和查杀。基于主动防御机制判定和中止可疑行为，并且结合诱饵文件防护、进程行为画像等功能可对具有勒索行为的程序进行发现和拦截；另外智甲可对文档的写行为进行判定，发现疑似恶意加密动作时可自动的在文档被破坏前进行主动备份，事后可通过文件恢复将用户损失降到最低。
探海 威胁检测系统	NDR 网络检测响应	在政企网出口、关键网段等位置旁路部署，可以作为云资源池部署。	探海基于网络流量感知和检测勒索攻击的活动，包括扫描、探测、钓鱼邮件投放、远程木马植入、横向移动与 C2 的连接等，并基于流量侧的协议解析和还原，捕获攻击载荷，调用安天 AVL SDK 反病毒引擎进行更精准的检测，从而能更提前发现勒索攻击的网络侧活动，联动响应和处置。
捕风 蜜罐系统	威胁欺骗捕获	支持企业内网、隔离网、私有云、公有云等部署场景。	捕风蜜罐系统支持通过系统和应用的模拟欺骗捕获威胁攻击，可以与导流设备结合，有效感知扫描探测、暴力破解、漏洞攻击、内网横向扩散和载荷投放等，从而把勒索攻击吸引到蜜罐中，快速发现勒索事件和情报，联动响应和处置，以供用户及时防御阻断勒索威胁传播。
追影 威胁分析系统	FA 文件分析	旁路部署，联动设备与查询结果终端路由可达即可。	追影可以与智甲、探海等安天全线产品联动使用，或安全工程师手工交互，基于深度静态分析和高仿真沙箱环境执行双重机制分析文件对象，针对勒索攻击文件载荷，可以有效分析标定漏洞利用、权限提升、防御对抗、文件加密与备份禁用等行为，协助用户生产威胁情报，联动威胁响应和处置。
拓痕 应急处置工具箱	应急处置	基于 U 盘、光盘、便携设备与场景连接使用。	拓痕基于对终端侧系统进行威胁检测分析，包括进程、服务、内核、引导扇区等对象的全要素的提取解析，调用安天 AVL SDK 反病毒引擎进行更精准的检测，检出和留存攻击载荷，提取可疑对象。从而有效发现勒索攻击在端点侧的活动，并通过底层处置能力，清除勒索软件实体与启动链，完成威胁发现、分析、取证、处置业务闭环。



图 4 安天勒索应急响应页面截图



图 5 安天勒索风险检测响应工具界面



图 6 安天杀毒软件界面

安天垂直响应平台中开通了面向 Windows 主机提供了勒索应急响应专题，用户可实时搜索勒索软件解密与相关应急信息。

详情地址：<https://vs.antiy.cn/fanlesuo>

以及轻量级勒索风险检测响应工具，帮助用户快速排查风险。

详情地址：<https://vs.antiy.cn/endpoint/rdt>

同时，个人和家庭用户，推荐安装使用安天杀毒软件（Windows 版），获得有效安全防护。

详情地址：<https://vs.antiy.cn/endpoint/anti-virus>

3. 安天安全服务中心勒索响应服务简介

勒索响应服务是基于经验丰富的专家团队与自主研发的安全产品构建形成的成熟服务体系，专家团队由身经百战的应急响应服务团队与高级威胁分析专家进行后端技术支撑组成全面的人员体系，7*24 小时服务响应，通过专家团队技术能力与拓痕应急响应工具包，快速发现问题根源，第一时间遏制勒索病毒传播，降低用户经济损失与负面的社会影响；通过应急响应团队搭配安天智甲终端防护系统对网内其他终端进行安全加固与风险排查，杜绝攻击者二次入侵，保障用户网内业务正常生产；结合威胁情报与渗透测试能力根据用户需求对勒索事件进行分析溯源。

安天部分历史公开勒索攻击相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
1	“攻击 WPS 样本” 实为敲诈者	https://www.antiy.com/response/CTB-Locker.html	2015-04-30
2	揭开勒索软件的真面目	https://www.antiy.com/response/ransomware.html	2015-08-03
3	邮件发送 js 脚本传播敲诈者木马的分析报告	https://www.antiy.com/response/TeslaCrypt2.html	2015-12-04
4	首例具有中文提示的比特币勒索软件 “LOCKY”	https://www.antiy.com/response/locky/locky.html	2016-02-19
5	勒索软件家族 TeslaCrypt 最新变种技术特点分析	https://www.antiy.com/response/TeslaCrypt%204/TeslaCrypt%204.html	2016-04-08
6	勒索软件 TeslaCrypt 再次来袭	https://www.antiy.cn/research/notice&report/frontier_tech/237.html	2016-04-17
7	修改 MBR 的敲诈者木马来袭	https://www.antiy.cn/research/notice&report/frontier_tech/239.html	2016-05-08
8	又见 Locky 家族勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/241.html	2016-05-22
9	勒索者与 DDOS 结合体样本分析	https://www.antiy.cn/research/notice&report/frontier_tech/242.html	2016-05-29
10	Rex 木马样本变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/559.html	2016-11-13
11	勒索木马 Shade 新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2017074.html	2017-01-22
12	勒索软件 KiDisk 分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017078.html	2017-03-05
13	安天移动安全《你可能下了个假的抢红包神器》	http://blog.avlsec.com/2017/03/4544/fake-red-packets/	2017-03-16
14	Cerber 勒索软件家族分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017085.html	2017-04-24
15	安天针对勒索蠕虫“魔窟”（WannaCry）的深度分析报告	http://www.antiy.com/response/wannacry.html	2017-05-13
16	安天应对勒索软件“WannaCry”配置指南	http://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html	2017-05-13
17	安天应对勒索者蠕虫病毒 WannaCry FAQ（1）	http://www.antiy.com/response/Antiy_Wannacry_FAQ.html	2017-05-13
18	安天应对魔窟勒索软件“WannaCry”周一开机指南	https://www.antiy.com/response/Antiy_Wannacry_Guide.html	2017-05-14
19	安天应对勒索者蠕虫病毒 WannaCry FAQ（2）- 传言验证者	https://www.antiy.com/response/Antiy_Wannacry_FAQ2.html	2017-05-14
20	安天对已感染勒索蠕虫“魔窟”（WannaCry）用户的重要建议	https://www.antiy.com/response/Antiy_Wannacry_Recover.html	2017-05-14
21	勒索蠕虫“魔窟”（WannaCry）FAQ（3）	https://www.antiy.com/response/Antiy_Wannacry_FAQ3.html	2017-05-14
22	安天关于“魔窟”（WannaCry）勒索蠕虫变种情况的进一步分析	https://www.antiy.com/response/Antiy_Wannacry_Explanation.html	2017-05-14
23	安天对勒索者蠕虫“魔窟”WannaCry 支付解密流程分析	https://www.antiy.com/response/Antiy_Wannacry_Pay.html	2017-05-17
24	安天针对攻击乌克兰等国的“必加”（PETYA）病毒分析与应对	https://www.antiy.com/response/petya.html	2017-06-29
25	CVE-2017-7925_漏洞分析报告	https://www.antiy.cn/research/notice&report/research_report/20170717.html	2017-07-17
26	Sorebrext 勒索软件样本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017096.html	2017-07-23
27	Mamba 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017101.html	2017-08-27
28	加强壳的 MBR 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017102.html	2017-09-03
29	新型 Bootlocker 勒索软件 RedBoot 分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017106.html	2017-10-01
30	坏兔子来袭，安天智甲有效防护	https://www.antiy.cn/research/notice&report/research_report/20171026.html	2017-10-26
31	勒索软件“ONI”分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017111.html	2017-11-12
32	Locky 勒索软件 asasin 变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017112.html	2017-11-19
33	新型勒索软件 GIBON 分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017113.html	2017-11-26
34	安天针对 VBA 宏勒索软件 BluFish 的检测分析与有效防护	https://www.antiy.cn/research/notice&report/research_report/20171130.html	2017-11-30

安天部分历史公开勒索攻击相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
35	勒索软件“Locky 变种 lukicus”分析披露	https://www.antiy.cn/research/notice&report/frontier_tech/2017114.html	2017-12-03
36	Locky 勒索软件 Discord Canary 变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2017115.html	2017-12-10
37	File-Locker 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018118.html	2017-12-31
38	2017 全球僵尸网络 DDoS 攻击威胁态势报告	https://www.antiy.com/response/Antiy-Global-Botnet-DDoS-Attack-Threat-Report-2017.html	2018-01-09
39	警惕 GlobelImposter 勒索软件，安天智甲有效防护	https://www.antiy.cn/research/notice&report/research_report/20180208.html	2018-02-08
40	GANDCRAB 勒索软件着眼“达世币”，安天智甲有效防护	https://www.antiy.cn/research/notice&report/research_report/20180228.html	2018-02-28
41	勒索“达世币”的 GANDCRAB 勒索软件更新 V2 版本，安天智甲有效防护	https://www.antiy.com/response/20180310.html	2018-03-09
42	勒索锁机木马 MBRLock 分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018128.html	2018-03-25
43	可卸载反病毒程序的勒索软件“AVCrypt”分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018129.html	2018-04-01
44	利用 Flash 0day 漏洞传播的勒索软件“Hermes”分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018130.html	2018-04-08
45	警惕首个卸载安全软件的勒索者“AVCrypt”	https://mp.weixin.qq.com/s/MZMCMUSacrFxOWEkRSVZXQ	2018-04-13
46	恶意代码下载器“QuantLoader”分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018131.html	2018-04-15
47	Samsam 勒索软件新变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018142.html	2018-07-01
48	GandCrab 勒索软件 V4 版本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018143.html	2018-07-08
49	Magniber 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018146.html	2018-07-29
50	“圣甲虫”勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018147.html	2018-08-05
51	Crysis 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018150.html	2018-08-26
52	GandCrab V5 勒索木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018154.html	2018-09-30
53	KeyPass 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018157.html	2018-10-28
54	Scarab 勒索病毒新变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018158.html	2018-11-04
55	GandCrab 勒索病毒变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018162.html	2018-12-02
56	Ryuk 勒索软件分析报告	https://www.antiy.cn/observe_download/observe_169.pdf	2019-01-07
57	Vidar 信息窃取木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019170.html	2019-01-27
58	Anatova 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019172.html	2019-02-24
59	FIN6 组织的针对性勒索软件攻击事件分析	https://www.antiy.cn/research/notice&report/research_report/20190509.html	2019-05-09
60	LockerGoga 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019184.html	2019-05-26
61	Shade 勒索病毒分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019185.html	2019-06-02
62	Sodinokibi 勒索病毒分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019186.html	2019-06-09
63	Maze 勒索病毒变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019187.html	2019-06-16
64	勒索软件 Sodinokibi 运营组织的关联分析	https://www.antiy.cn/research/notice&report/frontier_tech/2019186.html	2019-06-28
65	LooCipher 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019190.html	2019-07-07
66	DanaBot 木马变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019191.html	2019-07-14
67	ERIS 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019193.html	2019-07-28
68	Phobos 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019194.html	2019-08-04

安天部分历史公开勒索攻击相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
69	Nemty 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019198.html	2019-09-01
70	TFlower 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019202.html	2019-09-29
71	Phobos 勒索软件变种分析报告	https://www.antiy.com/response/20191016.html	2019-10-12
72	FTCode 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019206.html	2019-11-03
73	Major 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019208.html	2019-11-17
74	DoppelPaymer 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019209.html	2019-11-24
75	DeathRansom 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019210.html	2019-12-01
76	Rapid 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019211.html	2019-12-08
77	Montserrat 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019212.html	2019-12-15
78	Sifrelendi 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019213.html	2019-12-22
79	Mehdi 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019214.html	2019-12-29
80	Yarraq 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019215.html	2020-01-05
81	Ako 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019217.html	2020-01-19
82	Unique 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019218.html	2020-02-16
83	疫情防控期的几类网络安全威胁分析与防范建议	https://www.antiy.com/response/20200219.html	2020-02-19
84	Odveta 勒索软件变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019219.html	2020-02-22
85	Makop 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019220.html	2020-03-01
86	PwndLocker 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019222.html	2020-03-15
87	多起攻击工业企业的勒索软件 Ryuk 分析及防御建议	https://www.antiy.com/response/20200320.html	2020-03-20
88	利用疫情信息传播 KPOT 窃密木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019223.html	2020-03-22
89	传播 CoronaVirus 勒索软件和 KPOT 窃密木马事件的分析	https://www.antiy.com/response/20200323.html	2020-03-23
90	PXJ 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2020224.html	2020-03-29
91	Prolock 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2020225.html	2020-04-05
92	针对 WannaRen 勒索软件的梳理与分析	https://www.antiy.com/response/20200409.html	2020-04-09
93	Velar 勒索软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2020226.html	2020-04-12
94	勒索软件 ProLock 藏身图片，安天智甲有效防护	https://www.antiy.com/response/20200419.html	2020-04-19
95	安天智甲有效防护 Revon 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020227.html	2020-04-19
96	安天智甲有效防护 WANNACASH NCOV 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020228.html	2020-04-26
97	安天智甲有效防护 Snake 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020231.html	2020-05-24
98	安天智甲有效防护 Buran 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020232.html	2020-05-31
99	从反恶意代码到对抗高级威胁	https://www.antiy.com/response/20200615.html	2020-06-15
100	安天智甲有效防护 Hakbit 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020237.html	2020-07-05
101	安天智甲有效阻断 MedusaLocker 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020237.html	2020-07-19
102	安天智甲有效阻断 VoidCrypt 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020241.html	2020-08-02

安天部分历史公开勒索攻击相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
103	安天智甲有效防护 WastedLocker 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020242.html	2020-08-09
104	安天智甲有效防护 Tellyouthepass 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020243.html	2020-08-16
105	2020 版 Smokelocker 僵尸网络变种分析	https://www.antiy.cn/research/notice&report/research_report/20200821.html	2020-08-21
106	安天智甲有效防护 “Conti 勒索软件”	https://www.antiy.cn/research/notice&report/frontier_tech/2020244.html	2020-08-23
107	安天智甲有效阻断 DaVinci 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020245.html	2020-08-30
108	安天智甲有效阻断 Zeppelin 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020246.html	2020-09-06
109	安天智甲有效阻断 AIDS NT 2020 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020247.html	2020-09-13
110	安天智甲有效防护 ILMWL 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020248.html	2020-09-20
111	安天智甲有效防护 Zhen 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020249.html	2020-09-20
112	安天智甲有效防护 Badbeeteam 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020250.html	2020-10-18
113	安天智甲有效防护 Woodrat 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020251.html	2020-10-25
114	安天智甲有效防护 Pizhon 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020252.html	2020-11-01
115	安天智甲有效防护 Jdyi 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020253.html	2020-11-08
116	安天智甲有效防护 RegretLocker 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020254.html	2020-11-15
117	安天智甲有效防护 Dharma 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020255.html	2020-11-22
118	安天智甲有效防护 VoidCrypt 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020256.html	2020-11-29
119	安天智甲有效防护 Xorist 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020257.html	2020-12-06
120	安天智甲有效防护 BitRansomware 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020258.html	2020-12-13
121	安天智甲有效防护 Scarab 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2020259.html	2020-12-20
122	安天智甲有效防护 Kobos 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020260.html	2020-12-27
123	安天智甲有效防护 MountLocker 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2020261.html	2021-01-03
124	安天智甲有效防护 BabukLocker 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021262.html	2021-01-10
125	安天智甲有效防护 Saher Blue Eagle 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021263.html	2021-01-17
126	安天智甲有效防护 Encrptar 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021264.html	2021-01-24
127	安天智甲有效防护 TeslaRVNG 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021265.html	2021-01-31
128	首个 D 语言勒索软件，安天智甲有效防护	https://www.antiy.com/response/20210226.html	2021-02-26
129	安天智甲有效防护 Makop 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021267.html	2021-02-28
130	安天智甲有效防护 BleachGap 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021268.html	2021-03-07
131	RTM 团伙攻击活动利用新的 Quoter 勒索软件	https://www.antiy.cn/research/respond/threaten_info/2021269.html	2021-03-14
132	安天智甲有效防护 HelpYou 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021269.html	2021-03-14
133	通过 U 盘传播的多功能勒索软件分析	https://www.antiy.cn/research/notice&report/research_report/20210316.html	2021-03-16
134	安天智甲有效防护 DearCry 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021270.html	2021-03-21
135	安天智甲有效防护 Hog 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021271.html	2021-03-28
136	安天智甲有效防护 Matrix 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021272.html	2021-04-04

安天部分历史公开勒索攻击相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
137	安天智甲有效防护 WastedLocker 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021273.html	2021-04-11
138	安天智甲有效防护 Tellyouthepass 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021274.html	2021-04-18
139	2020 版 Smokelocker 僵尸网络变种分析	https://www.antiy.cn/research/notice&report/frontier_tech/2021275.html	2021-04-25
140	安天智甲有效防护 “Conti 勒索软件”	https://www.antiy.cn/research/notice&report/frontier_tech/2021276.html	2021-05-02
141	安天智甲有效阻断 DaVinci 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021277.html	2021-05-09
142	安天智甲有效阻断 Zeppelin 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20210510.html	2021-05-10
143	安天智甲有效阻断 AIDS NT 2020 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20210511.html	2021-05-11
144	安天智甲有效防护 ILMWL 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021278.html	2021-05-16
145	安天智甲有效防护 Zhen 勒索软件	https://www.antiy.com/response/20210517.html	2021-05-17
146	安天智甲有效防护 Badbeeteam 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021279.html	2021-05-23
147	安天智甲有效防护 Woodrat 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20210528.html	2021-05-28
148	安天智甲有效防护 Pizhon 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021280.html	2021-05-30
149	安天智甲有效防护 Jdyi 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021281.html	2021-06-06
150	安天智甲有效防护 RegretLocker 勒索软件	https://mp.weixin.qq.com/s/I4u9KzcqTQgV0ambj6txeQ	2021-06-09
151	安天智甲有效防护 Dharma 勒索软件新变种	https://www.antiy.com/response/20210611.html	2021-06-11
152	安天智甲有效防护 VoidCrypt 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021284.html	2021-06-27
153	安天智甲有效防护 Xorist 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021285.htm	2021-07-04
154	安天智甲有效防护 BitRansomware 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021286.html	2021-07-11
155	安天智甲有效防护 Scarab 勒索软件新变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021287.html	2021-07-18
156	安天智甲有效防护 Kobos 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021288.html	2021-07-25
157	安天智甲有效防护 MountLocker 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021289.html	2021-08-01
158	安天智甲有效防护 BabukLocker 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021290.html	2021-08-08
159	安天智甲有效防护 Saher Blue Eagle 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20210812.html	2021-08-12
160	安天智甲有效防护 Encrptar 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021291.html	2021-08-15
161	安天智甲有效防护 TeslaRVNG 勒索软件变种	https://www.antiy.cn/research/notice&report/frontier_tech/2021292.html	2021-08-22
162	首个 D 语言勒索软件，安天智甲有效防护	https://www.antiy.cn/research/notice&report/frontier_tech/2021293.html	2021-08-29
163	安天智甲有效防护 Makop 勒索软件变种	https://www.antiy.com/response/20210918.html	2021-09-18
164	安天智甲有效防护 BleachGap 勒索软件	https://www.antiy.cn/research/notice&report/frontier_tech/2021296.html	2021-09-19
165	RTM 团伙攻击活动利用新的 Quoter 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20211220.html	2021-12-20
166	安天智甲有效防护 HelpYou 勒索软件	https://www.antiy.cn/research/notice&report/research_report/20220103.html	2022-01-03
167	通过 U 盘传播的多功能勒索软件分析	https://www.antiy.cn/research/notice&report/research_report/20220222.html	2022-02-22
168	安天智甲有效防护 DearCry 勒索软件	https://www.antiy.com/response/20220323.html	2022-03-23
169	安天智甲有效防护 Hog 勒索软件	https://www.antiy.com/response/20220624.html	2022-06-24
170	安天智甲有效防护 Matrix 勒索软件新变种	https://www.antiy.cn/research/notice%26report/research_report/20220712.html	2022-07-12

“挖矿”威胁治理专项方案

02 “挖矿”威胁治理

“挖矿”威胁治理，既具备符合国家、相关行业的标准和规范的合规价值；亦能因此构建一体化安全管理闭环，提升安全运营能力；更能为推动国家节能减排，实现碳达峰、碳中和目标做出积极贡献。

随着技术的发展，如今，面临“挖矿”威胁传播方式多元、迭代变种迅猛、持久化手段丰富及黑灰产业链作业等严峻形势，治理策略不能采用传统的针对单一维度的考虑，而是需要进行纵观全局的多维度考量，进而制定动态综合的系统型解决方案。

本章内容将围绕专项方案，为用户提供有效治理策略；围绕产品能力，为用户提供有效产品决策；提供防护手册，为用户提供实战运营参考。

在此，感谢安天 CERT，解决方案中心马超、毛力伟，端点安全部李培涛，流量安全产品中心汤建平等对本章内容的所做出的贡献。



扫描二维码，观看专题视频

1. “挖矿”威胁行为与风险分析

2017 年 6 月，安天提出了“有效敌情想定是网络安全工作的前提”，将“敌情想定”这一军事术语引入了网络安全领域。在后续的实践中，安天以此为基础发展出“威胁想定分析框架”，作为重要信息系统和关键信息基础设施防护规划的基本方法。分析框架从“威胁行为体”、“动机”、“行为”、“资产环境”和“后果”等方面，围绕价值资产，分析关联的威胁行为体及其动机，根据历史案例和动机遍历威胁技术，分析威胁技战术对资产环境的影响以及风险后果，以此作为规划安全能力建设要点的需求输入。

安天 CERT 梳理了典型“挖矿攻击活动”的威胁行为及分析后果图谱。如图 2 所示。

综合来看，伴随加密应用的普遍化，“挖矿类”网络通信行为也隐藏在正常的加密通信中，传统边界侧安全的作用正在被削弱甚至被绕过，网络安全防护的支点重回系统侧安全；另外一方面，无论是内部人员自主行为、还是被攻击者入侵后的被动行为，“挖矿动作”的作用主体在主机节点，因此“挖矿”威胁治理工作的核心是需要加强对各类工作负载端点的统一管理，形成端点有效防护屏障。

同时，“挖矿”行为的主要动机是趋利行为，虚拟

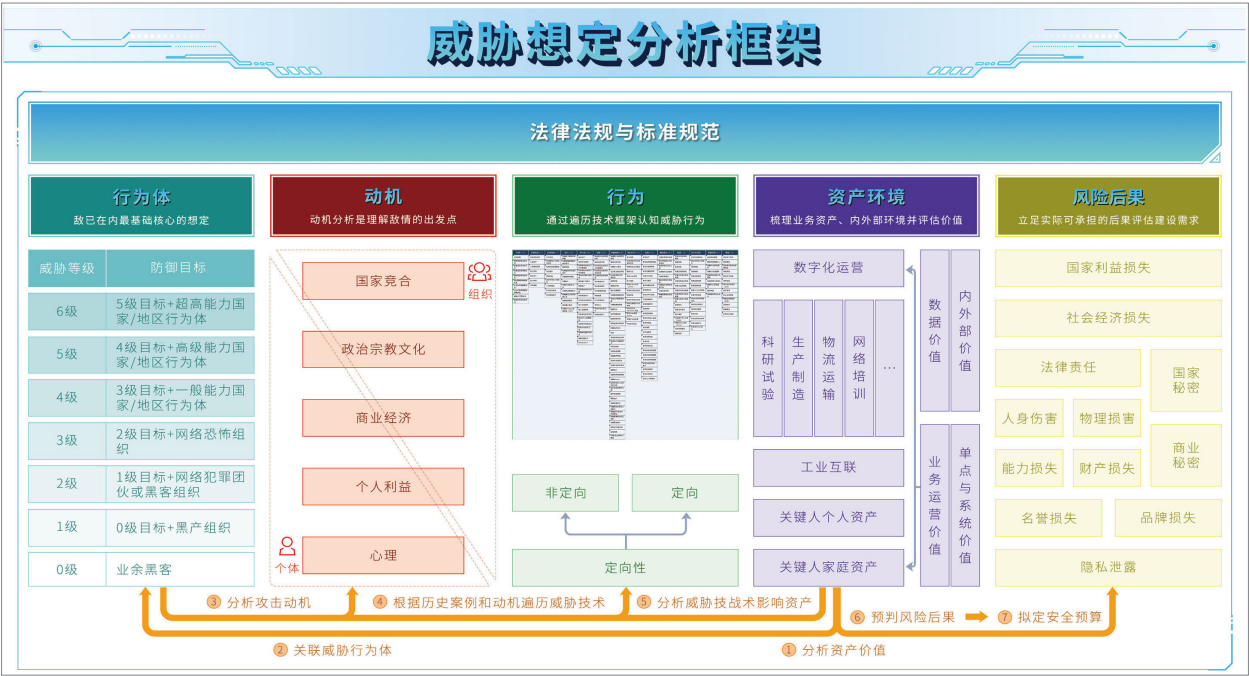


图 1 安天威胁想定分析框架

针对“挖矿”威胁攻击，理清“我情”（价值资产）、“敌情”（威胁行为体、动机、行为）、“风险后果”，是开展专项治理工作的前提。基于对典型“挖矿”攻击持续深度监测分析与赋能客户现场应急响应处置经验，

货币只要有利可图，“挖矿”威胁将持续存在，因此针对网内可能出现的主动或被动“挖矿行为”，还需要加强常态化安全监测和提升对“挖矿威胁情报”的消费能力，支撑更加及时和准确的检测与响应。

威胁行为体	动机	行为	资产环境	风险后果
内部员工	【心理】个人心理得到满足（报复、炫技或挑衅等）	主动下载挖矿软件	邮件系统	敏感信息泄露
个体黑客	【个人利益】通过挖矿，获得经济利益	利用扫描工具发现存在漏洞的网络主机	内网办公系统	影响业务系统稳定运行
黑客组织	【个人利益】毁坏目标形象	通过钓鱼邮件、弱口令破解或其他自动化手段获取主机控制权限	对外业务系统	浪费大量算力、能源，造成经济损失
一般行为体	【商业经济】通过挖矿，获得经济利益	钓鱼邮件、钓鱼网站、身份仿冒等社工形式获取管理员信息等	私有云主机	影响企业形象
	【商业经济】打击目标核心竞争力	网站挂马，入侵访问主机	物理服务器	个人经济损失
	【商业经济】干扰目标正常运行	SSH 暴力破解，传播挖矿木马	公有云相关资源	成为跳板机攻击其他计算资源
	【商业经济】通过挖矿，获得经济利益	获取访问权限，横向传播	研发终端	
	【国家竞合】打击目标生产交付体系	远程控制，下载挖矿软件	财务终端	
	【国家竞合】长期潜伏	DDoS 攻击或释放勒索病毒瘫痪服务器	办公终端	
		隐藏进程，替换、伪装系统进程，清除系统日志，欺骗检测排查		

图 2 典型“挖矿攻击活动”的威胁行为及分析后果图谱

2. “挖矿”威胁专项治理方案

通过多年的安全合规建设拉动，大部分政企单位已经形成了相对全面的防御纵深，针对“挖矿”威胁的专项治理工作，安天提出“端点统管、持续监测、情报驱动、协同响应”的总体思路，重点对客户侧现有防护体系进行加强、完善和统管，辅以流量侧的持续监测与端点侧防护形成互补。通过威胁情报的消费与运营支撑客户侧发挥传统安全设施的效能，并提供全方位的应急响应服务协同客户快速响应处置相关事件。



图 3 安天“挖矿”威胁治理体系架构

2.1 端点统管·构建系统侧有效防护能力

安天面向服务器、云、虚拟化、容器和传统办公节点等提供有全防御能力覆盖的“智甲安全产品家族”，可以满足客户对于包括终端杀毒、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求。

“智甲终端防御系统”是业内率先采用“云查杀+黑白双控模式”进行有效防御的终端安全防护产品，结合本地的深度检测和云端服务的强大计算能力，有效保障“挖矿木马”快速精准的识别，同时大幅减少终端资源占用；智甲能主动对进入系统的文件进行监控，自动感知并扫描文件安全性；自动扫描监控进程源文件以及调用文件的安全性；监控网络的端口和流量，实现对“挖矿行为”的实时监测告警。



图 4 智甲对“挖矿”的检测和查杀

2.2 持续监测·提升网络侧挖矿检测能力

通过部署“安天深海威胁检测系统”，对用户网络侧流量进行实时检测；深海基于内置的威胁检测引擎（文件检测引擎、C&C 检测引擎、网络行为检测引擎、自定义检测引擎）能够对采集到的数据从数据流、网络行为、文件等多层次进行检测，及时发现网络中的“挖矿木马”、病毒横向移动、病毒感染传播等攻击行为。

深海内置矿池相关威胁情报，可有效发现比特币、以太坊、门罗币、莱特币等主流的虚拟货币矿池连接行为，发现矿池“挖矿”活动；能够检测多种基于区块链的数字虚拟代币发行服务的矿池连接行为，可检测基于波场公链 TRON、币安智能链 BSC、火币生态链 HECO、以太坊 ETH 等公链发行的衍生虚拟货币。同时，通过对“挖

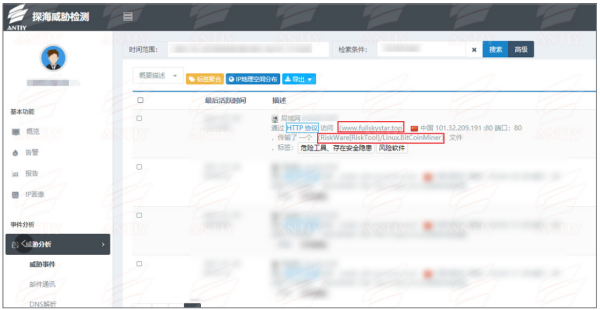
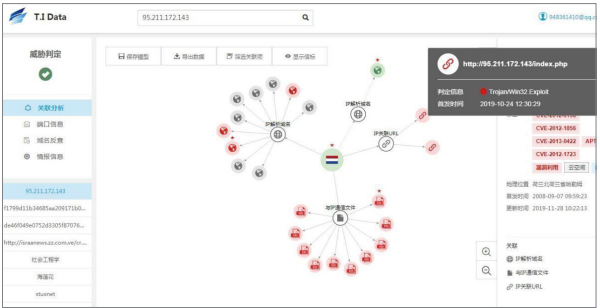


图 5 “挖矿”行为检测分析

矿”协议的分析与识别，在威胁情报滞后更新的情况下，也能发现在主要矿池进行的“挖矿”行为。

2.3 情报驱动·支撑智能化安全运营闭环

通过“安天威胁情报分析平台”、“追影威胁分析系统”和“捕风蜜罐系统”的威胁情报能力，有效提升客户情报赋能和私有化情报生产能力，可以有效支撑更为细致的“挖矿”活动分析工作，针对攻击者的攻击工具、攻击资源、攻击手段进行全面揭示，基于情报驱动网内各环节检测和发现能力。



有效实现对“挖矿”行为的实时监测告警、响应处置。

2.4 协同响应·协助快速处置与威胁猎杀

安天提供安全服务专家，通过远程或现场安全实时监测、响应处置和威胁猎杀服务，全面监测发现“挖矿行为”，检测内部失陷的主机，以及针对发现的“挖矿行为”进行分析研判，协助客户对疑似“挖矿主机”进行检查分析，对发现的“挖矿活动”进行彻底清除，并对相关“挖矿活动”进行深度分析和追溯，及时修复相关安全漏洞，避免主机被再次植入“挖矿程序”，做到把“挖矿活动”“找出来”和“赶出去”。

3. “挖矿”威胁治理价值

合规价值：全面梳理排查虚拟货币“挖矿”威胁，符合国家、相关行业的标准和规范，以及主管部门监管检查要求。

运营提升：从“端点统管、持续监测、情报驱动、协同响应”四个维度入手，构建挖矿木马检测、防护、监测、研判、溯源和取证一体化安全管理闭环，提升安全运营能力，确保企业内的“挖矿”行为无处藏身。

社会效益：积极响应国家政策，有效防护和清除“挖矿”活动，降低“挖矿”能源和计算资源消耗，为推动国家节能减排，实现碳达峰、碳中和目标等做出积极贡献。

智甲构建系统侧有效防护

“智甲安全产品家族”面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖，可以满足客户对于包括终端杀毒、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求。

1. 特征检出

“智甲终端防御系统”是业内率先采用“云查杀+黑白双控模式”进行有效防御的终端安全防护产品，结合本地的深度检测和云端服务的强大计算能力，有效保

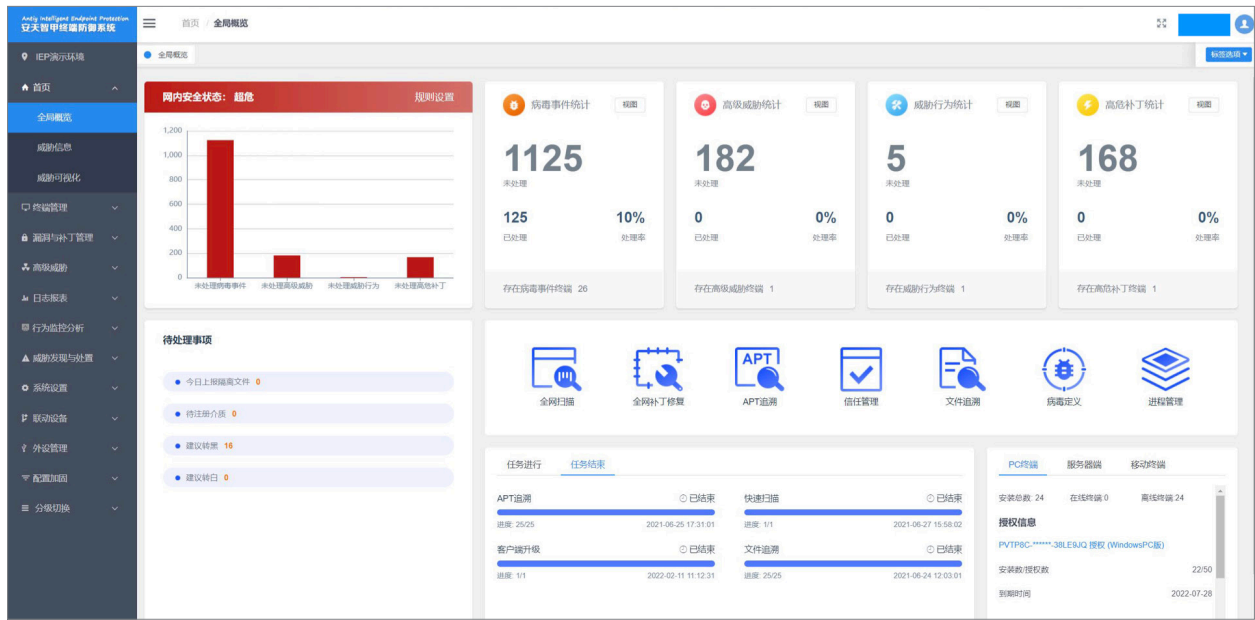


图 1 智甲终端防御系统端点统管控制台截图



图 2 智甲应对“挖矿”威胁时的防护方案

障“挖矿”木马快速精准的识别，同时大幅减少终端资源占用。

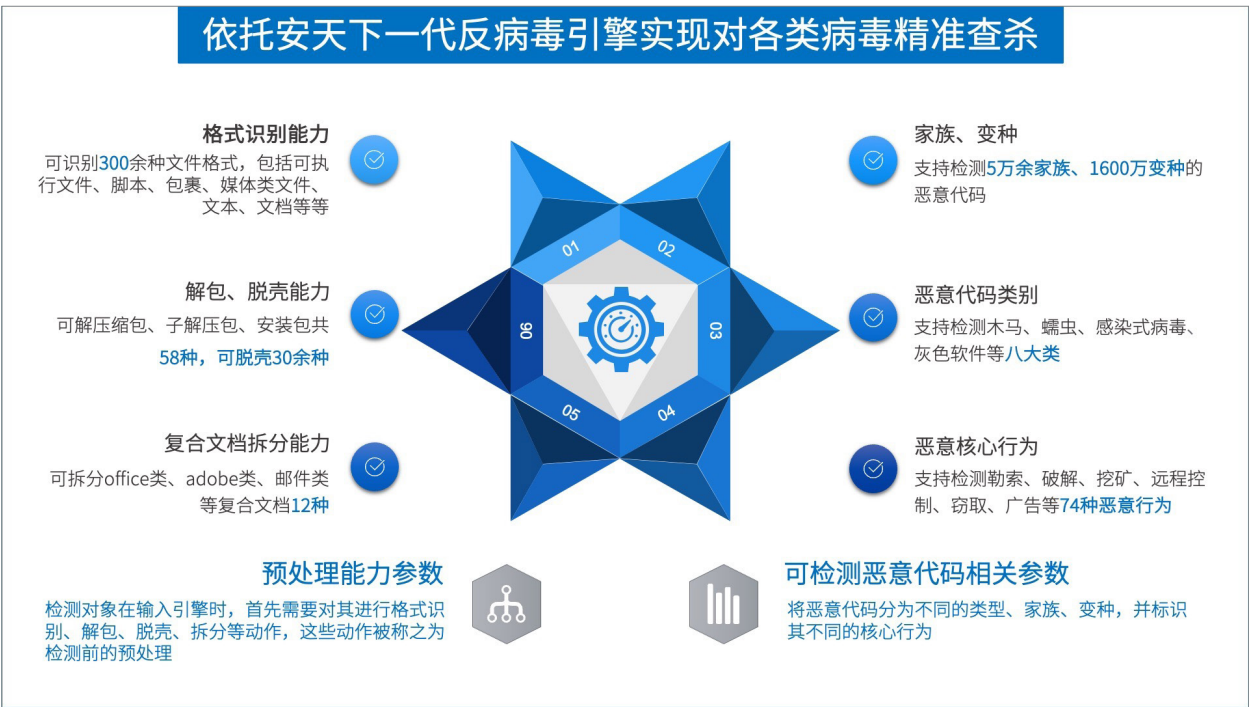


图 3 依托安天下一代反病毒引擎实现对各类“挖矿”木马精准查杀

通过云查杀，在环境受限的情况下，智甲客户端无需在本地加载体积庞大的病毒库（本地客户端具有流行库，离线后仍具有一定的查杀能力），即可达到良好的查杀效果，同时在进行全盘扫描时，不会造成终端负载过高的现象，保证终端扫描时，其他办公业务能够稳定运行。

通过多引擎、多维度检测分析，快速高效查杀已知“挖矿”木马、已知“挖矿”木马变种以及未知“挖矿”木马的同时，深度揭示文件静态向量，辅助人工判定。在没有网络不依赖云端病毒特征库情况下，仍可强力查杀威胁。

2. 行为阻断

2.1 文件防御

智甲可实时检测、捕获“挖矿”木马文件并防止传播。对终端关键目录进行实时监控，当感知到有新增文件时，会自动获取文件的特征，如 MD5、文件路径、文件名称等，并将这些信息投递给本地或者服务端反病毒引擎进行病毒检测，如果检测出新增文件为恶意文件，则会立即进行告警，并支持自动或者手动处置恶意文件。

除了自动检测外，用户还可以通过快速扫描、全盘扫描、指定位置扫描等方式对终端文件进行检测，检测时系统会严格遵守三元权限要求，仅对自己有访问权限的文件进行检测与清除。

2.2 进程防御

智甲可感知到终端进程启动行为，在监测到有进程启动后，会自动获取进程源文件信息并将其投递给反病毒引擎进行检测，如果进程源文件判定为恶意，智甲会自动告警并拦截进程行为。在进程启动后，如果智甲检测到进程有可疑或者高危行为，同样能够告警并立即阻止进程行为。

2.3 病毒文件隔离

针对可执行文件类型的“挖矿”木马文件，智甲能够将文件加密并移动至病毒隔离区，加密后的“挖矿”木马文件无法启动运行，移动至病毒隔离区时，系统会

记录文件的源路径、MD5、文件 owner、权限、处理进程等信息。用户可通过客户端的人机交互界面对已隔离的文件进行彻底删除或者恢复至原路径。

同时支持主动检测外部输入文件，来源包括：

- 1) 接入设备：U 盘、网络磁盘、共享网盘、浏览器下载文件、即时通讯下载文件、邮件附件等进行主动查杀。
- 2) 外接设备：键盘、鼠标、USB 蓝牙适配器、USB 打印机、U 盘 / 移动硬盘 /SD 卡 / 移动光盘 / 软盘、HUB、USB 智能卡、USB 网卡和未识别设备。
- 3) 移动介质：可自动和手动注册移动介质，为移动介质设置终端设备访问权限，并提供移动介质操作审计日志，可追溯移动介质使用情况。

3. 程序清除

企业内网中一旦出现“挖矿”木马，由于交叉感染等原因很难彻底清除。传统的防病毒软件只能通过全网全盘查杀进行处置，但这种方式既耗时又影响正常业务的运行，尤其是针对端点数量在万点以上的网络，很难做到同一时间全网清除。

智甲可对企业内网中个体终端发现的“挖矿”木马文件进行全网追溯，每个终端无需耗时的全盘查杀，基于已发现的“挖矿”恶意代码攻击的特征，管理员可在企业全网终端中查找已知的“挖矿”威胁攻击，包括威胁攻击事件中利用的文件、注册表、数字签名等，为用户进行攻击溯源和取证提供依据。

企业内超过万点终端（无上限），全网追溯整个过程不超过 15 分钟，管理员即可快速定位全网感染同样“挖矿”木马的终端分布情况。针对这些病毒，管理员无需每台机器都人工逐个清除，在管理中心即可下发定点清除的指令，从而全面提升“挖矿”威胁防控的精准度和处理效率。

智甲可根据用户需求自定义事件进行定时病毒查杀。可通过客户端直接进行定时查杀任务设置，也可通过服务端向多台客户端进行定时查杀任务下发，客户端会对设置的定时任务进行自动处理。

病毒处理	支持对“挖矿”病毒文件进行删除或者仅告警等处理方式，删除病毒文件时支持隔离或者直接删除等方式，并支持在管理中心远程、批量清除全网终端上的指定病毒文件，支持远程、批量恢复终端隔离文件。
	支持导入威胁处置规则，当触发监控条件时，自动清除相应威胁。
全网病毒追查	支持全网病毒追溯功能，管理中心通过对指定“挖矿”病毒文件进行追查，可迅速评估病毒感染的范围、追查病毒的最初来源和传播路径，实现病毒可审计、可回溯，并可在管理中心远程清除全网终端上的该病毒文件。
威胁处置	支持通过管理平台清除指定终端上的未处理的“挖矿”病毒文件。
	支持采用自动或手动方式，按管理员自定义的时间周期清除未处理的病毒和未处理的高级威胁。
	支持动态威胁处置，对主动防御上报的威胁进行处置，包括单一终端和全网终端的处置 / 信任，对于处置错误的情况，支持还原处置规则。
	支持设置威胁自动处置策略，用于清除网内持续威胁；支持高危行为优先出处置策略，用于将防御日志中违规处置并且符合高危行为优先处置规则的数据将自动加入到动态威胁处置。

探海提升流量侧威胁洞见（附案例）

1. 持续监测·提升“挖矿”威胁治理检测能力

探海综合运用多重检测机制，可从流量侧对“挖矿”行为进行持续监测和分析，检测机制包括挖矿程序检测、挖矿通信行为检测、挖矿 IOC 威胁情报检测；从数据流、网络行为、文件等多层次多维度对“挖矿”威胁进行有效分析。

同时，可联动“安天追影威胁分析系统”进行深度分析，有效检出特种木马、变种木马和未知木马；联动“安天智甲终端防御系统”和防火墙对“挖矿”活动进行及时处置，达成“挖矿”威胁的全面检测及治理。

1.1 挖矿程序检测

探海依托安天 20 余年专业反病毒经验与能力积累，可精准告警“挖矿”木马；基于载荷还原检测技术，支持还原并检测邮件中的附件、URL，有效检出钓鱼恶意附件、钓鱼 URL 等“挖矿”威胁初始访问行为。

即使文件采取了压缩、加壳等新行为规避，也能及

时发现下载、站点托管下载器等行为，有效发现“挖矿”木马的防御规避行为。

1.2 挖矿通信行为检测

探海基于“挖矿”活动的通信协议特征，可有效发现网内远控活动迹象。在威胁情报滞后的情况下，也能有效检出“挖矿通信”行为。

同时，可根据“挖矿协议”检测不同阶段的“挖矿”行为，主要包括：登陆矿池行为、获取挖矿任务、提交挖矿进度、链接钱包等。支持对网内的 TCP SYN、ICMP 扫描等扫描行为的发现，检测包括“挖矿”活动在内的侦查、扫描行为；支持对弱口令暴力破解等方式进行的强力攻击检测，发现账户入侵行为；支持各类远程执行漏洞利用行为检测，发现“挖矿”木马的执行、提权等活动行为；并对横向移动过程中的主机发现行为、端口扫描行为、暴力密码猜解进行检测，有效发现此类横向移动传播方式。

1.3 挖矿 IOC 威胁情报检测

探海基于“挖矿”木马的命令与控制地址情报库，可识别网内尝试连接“矿池地址”和“挖矿木马远控地址”的行为，目前支持检测多种“挖矿木马家族”，如 Keylogger、Plugx、Dropper 等；支持的“挖矿”木马情报类型包括“挖矿木马家族”使用的 URL、IP、C2/ 矿池域名等；可有效检测“挖矿”木马的命令与控制常用技术，及时发现“挖矿”活动行为。

1.4 联动处置“挖矿”木马

针对“挖矿”木马的处置，探海主要包括以下几点联动处置方式：

- 1) 联动追影：深度分析，发现未知
可联动追影对探海还原的恶意文件进行深度分析，及时发现“挖矿”木马的虚拟化 / 沙箱逃逸、漏洞规避防御等行为，有效检出特种木马、变种木马和未知木马。同时，追影自动化生成的 C2 等情报规则可反馈到探海中，增强探海对未知“挖矿”木马的发现能力。
- 2) 联动智甲，协助取证，快速处置
根据探海威胁事件告警定位失陷主机，可联动智甲完成终端侧的取证及处置。同时，追影的 C2 情报等规则可同步到智甲进行终端侧“挖矿”木马的全面查杀，快速清除网内“挖矿”威胁。
- 3) 联动防火墙，及时阻断，降低损失
通过联动防火墙，可有效阻断内网主机与矿池域名进行通信行为，及时止损。

2. 三大优势，直击“挖矿”威胁治理实际痛点

2.1 多层次多维度检测，“挖矿”威胁有效发现

探海支持从数据流、网络行为、文件等多个层次对“挖矿”活动进行检测，综合运用 AVL、行为检测、威胁情报、模型分析、关联分析等多种检测手段，对处于不同攻击阶段的“挖矿”行为进行精准检测与告警，包括但不限于网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动等“挖矿”威胁攻击行为。可高准确率、低误报率的，快速发现“挖矿”威胁。

2.2 细粒度全要素留存，“挖矿”威胁有效分析

基于流量侧海量的威胁线索，如何做到有效溯源分析，是网络安全检测重要的一环。区别于全流量缓存记录的方式，探海基于流量侧的细粒度协议解析和还原，支持对网络元数据、应用层传输要素、载荷对象要素等信息进行全要素留存，为“挖矿”威胁攻击溯源提供更精准更全面的威胁线索。

同时，基于恶意代码传播关系、命令与控制关系、恶意文件关联等维度，进行网络侧威胁事件自动化关联分析，可更有效的支撑安全分析人员进行威胁研判、追踪溯源，提高“挖矿”威胁攻击分析效率。

2.3 多产品间协同联动，“挖矿”威胁有效处置

探海可无缝与智甲、追影等产品进行协同联动，系统构建网络侧和终端侧纵深防护体系，有效应对内网场景、远程接入场景、外部访问场景下，“挖矿”木马进驻系统或横向移动的行为。

案例：教育行业“挖矿”威胁治理场景价值

1. 及时发现威胁

在一次校园网重保期间，探海在流量侧检测到 50+ 台主机访问已知的矿池域名或访问相关 C2 域名 (见表 1)，共 7 万 + 起“挖矿”威胁事件告警 (见图 1)，持续多日检出“LaofuMiner ‘挖矿’木马”、“NRSMiner ‘挖

矿’僵尸网络”等多种“挖矿”威胁。安全分析人员通过探海目标审计功能 (见图 2) 对校园网内“挖矿流量”进行全流量溯源取证，确认 20+ 台主机存在执行获取任务、回传任务的“挖矿”行为，根据钱包地址获取到 6 台主机在“挖矿”门罗币 (见图 3 至 5)。

表 1 检出矿池域名与攻击次数统计 (部分)

探海检出结果	检出域名	攻击次数
Trojan/Win32.NSAGluptebaMiner(RAT)	t.awcna.com	549
Trojan/Win32.LaofuMiner(RAT)	t.tr2q.com	1207
Trojan/Win32.WatchBogMiner(RAT)	sadan666.xyz	18
Trojan/Win32.NRSMiner(RAT)	null.exhaust.com state.codidled.com take.exhaust.com	71044
Trojan/Win32.MsraMiner(RAT)	tsk.tknv.com	3062
Trojan/Win32.StartMiner(RAT)	pool.supportxmr.com	1058



图 1 威胁事件告警，定位失陷主机



图 2 目标审计



图 3 涉及主机存在的异常网络行为



图 4 获取任务，回传任务进度

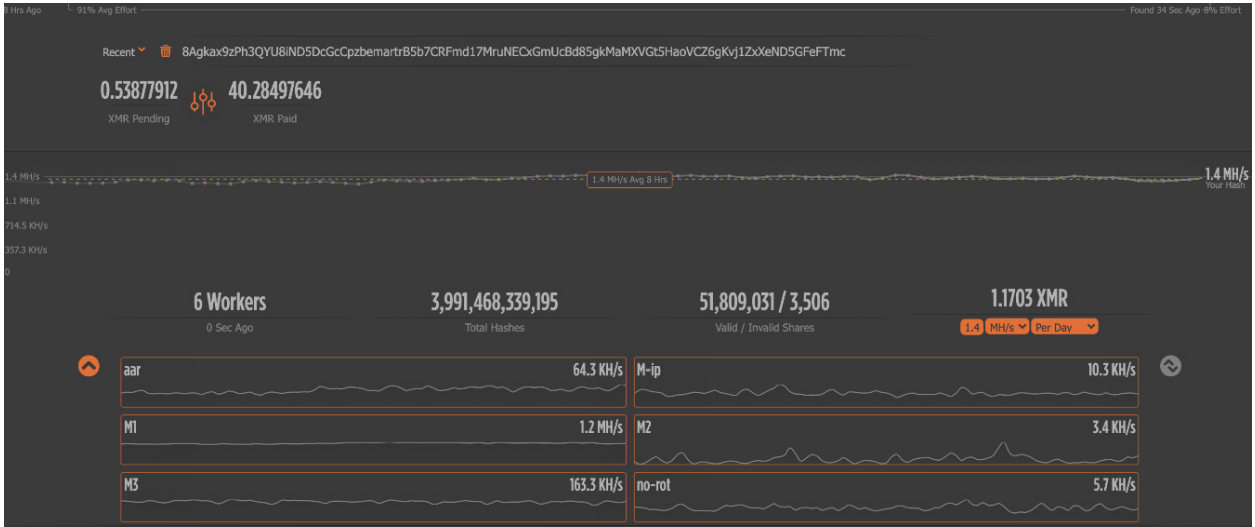


图 5 根据钱包地址获取到 6 台主机在挖门罗币

2. 快速联动处置

联动智甲协助用户完成了 20+ 台主机侧“挖矿”木马的查杀；同时联动防火墙对相关矿池域名进行阻断处理，阻断内网主机与矿池域名进行数据交换行为，成功处置了校园网内感染的“挖矿”木马。

3. 高效溯源反制

基于对网络元数据、应用层传输要素、载荷对象要素等信息的全要素留存，恶意代码传播关系、命令与控制关系、恶意文件关联等维度的网络侧威胁事件自动化关联分析，以及威胁事件日志及目标审计功能，有效地支撑了安全分析人员对该次“挖矿”活动的全面威胁研判与追踪溯源。

最终，高效的帮助用户回溯分析“挖矿”威胁攻击行为、还原攻击路径、分析感染影响状况，并及时修复了相关安全漏洞，避免主机被再次植入挖矿程序；做到了把“挖矿”活动“找出来”和“赶出去”，实现了对“挖矿”威胁的反制。

安天部分历史公开挖矿威胁相关报告简览（截至 2022 年 7 月）			
序号	报告标题	报告地址	发布时间
1	一款以 FTP 服务器为目标的蠕虫病毒分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/244.html	2016-06-12
2	2017 全球僵尸网络 DDoS 攻击威胁态势报告	https://www.antiy.com/response/Antiy-Global-Botnet-DDoS-Attack-Threat-Report-2017.html	2018-01-09
3	“挖矿”恶意代码肆虐，安天智甲有效防护	https://www.antiy.cn/research/notice&report/research_report/20180314.html	2018-03-14
4	使用“天堂之门”技术的挖矿木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018132.html	2018-04-22
5	FileTour 恶意广告软件分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018137.html	2018-05-27
6	ProximityUntilCache32.tlb 挖矿木马样本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2018160.html	2018-11-18
7	Johnnie 挖矿木马样本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019166.html	2018-12-31
8	Wirenet 木马样本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019169.html	2019-01-20
9	WebCobra 挖矿木马样本分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019171.html	2019-02-17
10	利用新型黑客工具传播挖矿木马活动的分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019174.html	2019-03-10
11	安天蜜网捕获“利用 Elasticsearch Groovy 漏洞进行门罗币 (Dog) 挖矿”事件分析	https://www.antiy.cn/research/notice&report/research_report/20190625.html	2019-06-25
12	ZombieBoy 挖矿木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019195.html	2019-08-11
13	Mykings 僵尸网络近期活动分析报告	https://www.antiy.com/response/20190822.html	2019-08-21
14	GroksterMiner 挖矿木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019197.html	2019-08-25
15	Beapy 挖矿木马分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2019199.html	2019-09-08
16	六小时处置挖矿蠕虫的内网大规模感染事件	https://www.antiy.cn/research/notice&report/research_report/20190925.html	2019-09-24
17	针对 WannaRen 勒索软件的梳理与分析	https://www.antiy.com/response/20200409.html	2020-04-09
18	精准投放 Tsunami 僵尸网络和“魔铲”挖矿木马的行动分析	https://www.antiy.cn/research/notice&report/research_report/20200424.html	2020-04-24
19	针对某云平台服务器的“云铲”挖矿木马事件分析	https://www.antiy.cn/research/notice&report/research_report/20210202.html	2021-02-02
20	挖矿木马简要技术分析	https://www.antiy.cn/research/notice&report/research_report/20211015.html	2021-10-15
21	z0Miner 挖矿木马变种分析报告	https://www.antiy.cn/research/notice&report/frontier_tech/2021299.html	2021-10-24
22	双平台传播——活跃的 H2Miner 组织挖矿分析	https://www.antiy.cn/research/notice&report/research_report/20211117.html	2021-11-17
23	冬训营 一例挖矿木马的应急响应	https://mp.weixin.qq.com/s/s9h1svYOa1x_-y4Iuq7uDg	2022-01-29
24	2021 年典型挖矿木马盘点	https://www.antiy.cn/research/notice&report/research_report/20220214.html	2022-02-14
25	“1337”挖矿组织活动分析	https://www.antiy.cn/research/notice&report/research_report/20220321.html	2022-03-21
26	“8220”挖矿组织活动分析	https://www.antiy.cn/research/notice&report/research_report/20220428.html	2022-04-28
27	活跃的 Kthmimu 挖矿木马分析	https://www.antiy.cn/research/notice&report/research_report/20220527.html	2022-05-27
28	活跃的 Hezb 挖矿木马分析	https://www.antiy.cn/research/notice&report/research_report/20220705.html	2022-07-05

03 攻防演练实战

大型网络实战攻防演练活动，旨在发现各行业重要信息系统的安全风险与隐患，考察网络安全责任落实情况，检验安全防护能力。近几年，通过持续的组织与推进，我国重要行业信息系统和关键信息基础设施的网络安全防护水平和技术对抗能力不断提高，应对相关突发事件的能力也得到提升。

为支撑用户更好地开展新形势下攻防演练活动，构筑动态综合的防御体系，本章内容从防守要点、各阶段 / 场景化专项防护方案、终端 / 云主机防护、全流量威胁检测、文件分析、欺骗式防御 / 威胁捕获、边界阻断与入侵防护等维度展开，综合分享实践经验、产品创新与场景价值，提供系统解决方案参考。

在此，感谢安天 CERT，安全服务中心尹尚书、张耀林，端点安全部李培涛、陈浩，流量安全产品中心汤建平，威胁情报产品中心靳山，欺骗防御产品中心康学斌、曾鸿林，青竹智语实验室刘志辉、徐郢，产研管理中心许鹏飞等对本章内容的所做出的贡献。



扫描二维码，观看专题视频

攻防演练防守要点与解决方案

构筑动态综合的防御体系，是保障攻防演练防守效果的基础前提；同时，有效的防御体系，既能从时间维度上横向支撑起攻防演练活动的每一个阶段，亦可从场景化维度纵向深入到威胁情报、靶标安全、欺骗式防御等专项防护。进而形成有效的协同联动机制，达成攻防演练防守的全场景实战赋能，实现少丢分甚至多加分。

本章内容将分享安天基于防守要点全面支撑启动阶段、准备阶段、决战阶段、总结阶段等四个阶段，有效帮助用户做好全面防护的解决方案。

1. 十大防守要点

在攻防演练对抗中，攻击方以防守方的靶标系统为

最终攻击目标。首先，是从防守方网络外围逐步向内渗透，通过对暴露在互联网的网站、邮箱、OA 等信息进行攻击获取控制权；其次，再对目标内部网络进行横向渗透，获取更多的业务系统、办公终端、网络设备与安全设备的权限；最终，实现攻陷，以达成攻击目的。

基于 20 余年持续参与重大应急响应支撑的专业积淀，安天连续多年在攻防演练期间为国家部委、能源电力、交通运输、金融、大型国企等客户执行防守任务，有不丢分、多加分的实战防护经验，为客户带来安全价值提升和安全信誉。安天综合梳理了自己以及其他防守方经验，特别针对常见的丢分点，总结出了十项防守要点：

安天攻防演练十大防守要点综述表		
序号	易丢分点	防守要点
1	互联网资产范围不清晰，开放过多敏感端口，管理后台未做好访问控制；	资产暴露面管控
2	信息系统存在安全漏洞和弱口令情况，被攻击方利用后获取权限；	系统漏洞管理
3	网络边界缺乏有效安全管控和监测措施，攻击方很容易突破进行横向移动；	网络边界监测与防御
4	缺失对所有主机统一安全管理防护，被攻击方突破后植入木马进行远程控制；	端点安全统管
5	缺乏有效威胁情报来源，对已暴露的攻击手段和最新漏洞无法及时获悉；	专项威胁情报
6	缺少可以迷惑攻击方、延缓攻击、溯源加分的诱饵系统；	欺骗式防御构建
7	靶标系统防护强度不够，被攻击方进入内网后攻陷；	靶标安全防护
8	员工安全意识薄弱，容易被攻击方社工钓鱼邮件攻击；	安全意识宣贯 & 攻防预演
9	供应链存在风险隐患，容易被攻击者利用进行突破；	供应链安全管控
10	防守队伍安全技术能力不足，在对抗过程中无法精准定位、分析溯源与处置威胁。	安全专家支撑

2. 覆盖全生命周期的解决方案

安天针对防守要点，结合自主安全产品，解决方案能全面支撑攻防演练全生命周期的四个阶段。

击手段，全面提升相关人员的防护水平。

最后，在演练活动正式开始前，协同用户制定演练期间的值守方案，确保值守方案可有效落地执行；在演



图1 安天攻防演练全生命周期解决方案

2.1 启动阶段

演练启动阶段，安天将基于用户场景进行资产梳理和网络安全防护现状调研，协助用户建立健全攻防演练组织和管理规划，明确演练期间的各项工作机制，向所有相关责任人宣贯攻防演练的重要性和工作部署方案。

同时，对用户的网络安全架构进行评估，给出优化方案。

2.2 准备阶段

首先，组织专项团队为用户提供脆弱性检测服务，检测方法包括基线检查、漏洞扫描、渗透测试等，并在完成检测后，为用户提供安全加固服务，协助对存在漏洞和不安全配置的资产进行全方位的安全加固；同时依据安全现状进行安全防守策略调优，提升安全产品对抗强度。

其次，是同步进行威胁检测与处置，及时检查并处置主机上的木马病毒。

此外，将为用户提供安全意识、安全攻防技术等安全培训，帮助相关人员识别演练中攻击方常用的各种攻

练活动临近时，组织多场景的攻防预演，以此验证安全加固和优化工作的有效性、各项工作机制的可操作性、以及各防守成员间的协作配合程度。

2.3 决战阶段

安天将基于自身的威胁情报分析平台和威胁捕获系统为用户提供威胁情报服务，协助用户全方位掌握演练活动期间的相关威胁情报。同时，利用自研安全产品和用户已有的第三方安全产品，为用户提供 7×24 小时的安全监测值守服务，包括专项威胁情报、邮件安全监测、网站安全防护、靶标安全防护、网络边界监测、终端威胁检查、欺骗式防御等专项服务。

演练值守期间，组织专项团队对安全告警和威胁情报等进行分析确认，在确认发现安全事件时，如防线被攻方团队攻破、信息破坏（篡改、泄露、窃取、丢失等）、大规模病毒、远控木马、网站漏洞事件等，安天将及时进行事件分析与应急处置，并协调相关资源进行追踪溯源，协助用户撰写防守成果报告，报送给相关单位，获得加分。

2.4 总结阶段

演练结束后，将对演练期间攻击成功的事件和防守成功的事件等相关情况，进行详细的全过程复盘；同时，基于演练过程中的工作记录，总结与安全事件相关的各种信息，根据演练工作中暴露的安全问题和流程问题，

为用户提供针对性的措施和建议，并协助用户完善安全防御机制，优化网络安全防护体系。

最后，安天还将为用户提供具有针对性的专项技能培训服务，协助用户培养自身的网络安全人才体系。

攻防演练七大场景化专项防护

1. 七大场景化专项防护

1.1 专项威胁情报

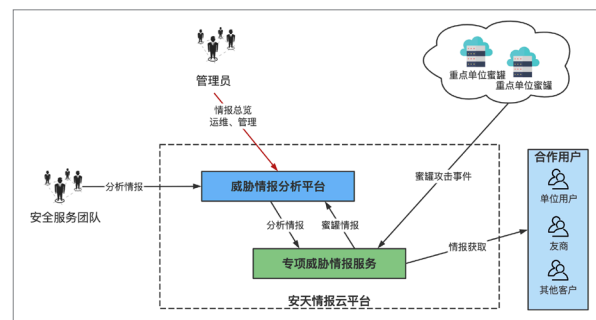
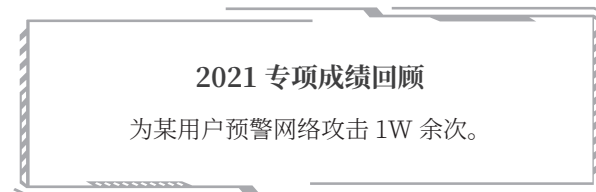


图 1 专项威胁情报服务

演练期间，安天将为用户提供实时最新汇聚的攻防演练威胁情报，情报内容包括攻击 IP 情报、最新漏洞情报、攻击手法情报等，协助用户提前做好安全加固和防御阻断。

同时，安天还将利用演练中发现的威胁线索在安天威胁情报分析平台上拓线查询，帮助分析人员溯源并得分。演练结束后，全面总结威胁情报工作成果，输出《专项威胁情报总结报告》。



1.2 邮件安全监测

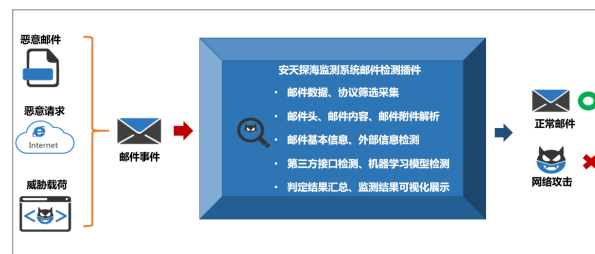
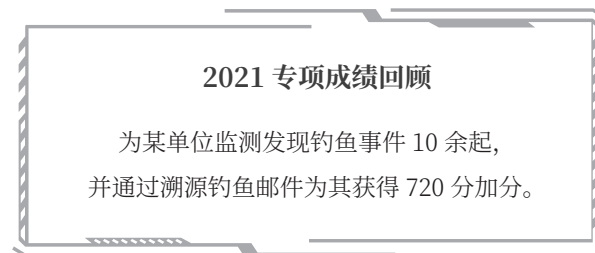


图 2 邮件安全监测服务

演练前，部署带有钓鱼邮件监测模块的安天探海威胁检测系统。

演练期间，通过邮件安全监测服务，发现社工邮件、发现网络入侵、处置已获得桥头堡、追溯攻击，开展深度分析和应急处置并形成分析报告，上报演练指挥部，获得加分。

演练结束后，全面总结演练期间邮件安全监测工作及成果，输出《邮件安全监测总结报告》。



1.3 网站安全防护

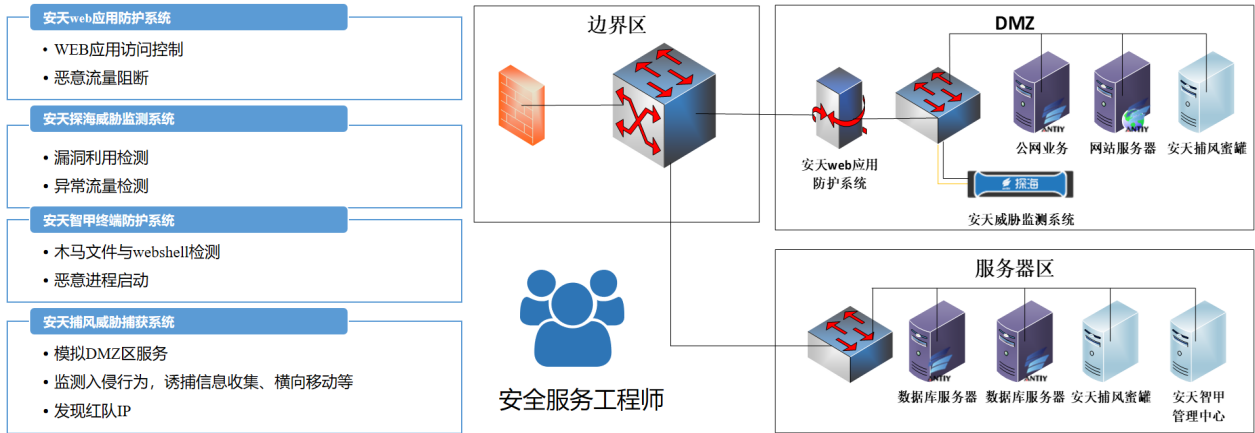


图3 网站安全防护服务

演练前，对网站资产进行暴露面梳理，尽量收窄暴露面。开展安全基线检查、漏洞扫描和渗透测试，发现网站存在的安全漏洞，协助用户进行安全加固；部署Web应用防护系统、安天探海威胁检测系统进行防御。

演练期间，通过两款安全产品监测并分析研判网络攻击事件，对攻击IP及时进行封禁阻断，对入侵事件及时应急处置并分析溯源形成分析报告，上报演练指挥部，获得加分。

演练结束后，针对演练期间发现的网站攻击事件进行汇总，输出《网站安全防护总结报告》。

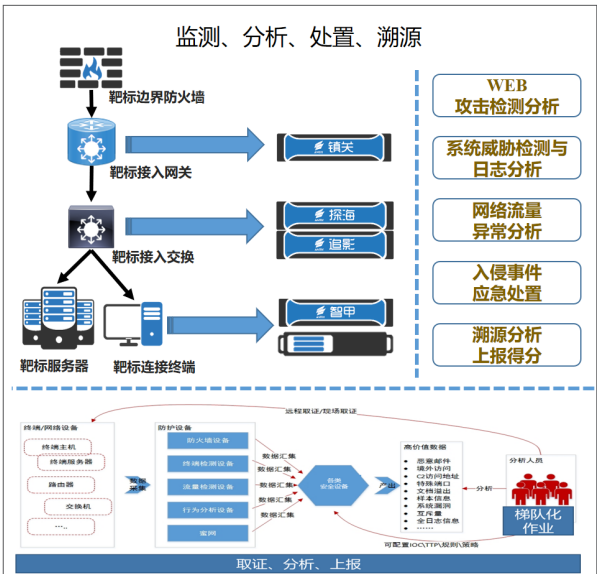
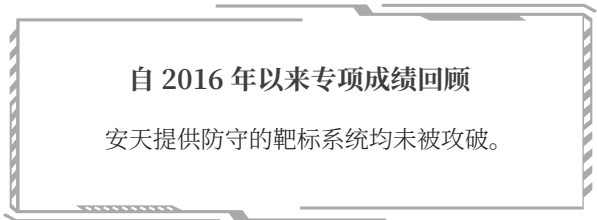


图4 靶标安全防护服务

演练结束后，全面总结演练靶标防护工作和成果，输出《靶标防护总结报告》。



1.4 靶标安全防护

演练前，协助用户做好靶标系统的全面资产、配置、漏洞、补丁梳理工作，并进行全面的风险排查，确保在演练前发现潜在风险并做好安全加固。

演练期间，安排监测分析人员7*24小时值守，做好针对靶标系统的威胁监测、研判、处置等工作，及时阻断威胁，提取并分析攻击证据，上报演练指挥部。

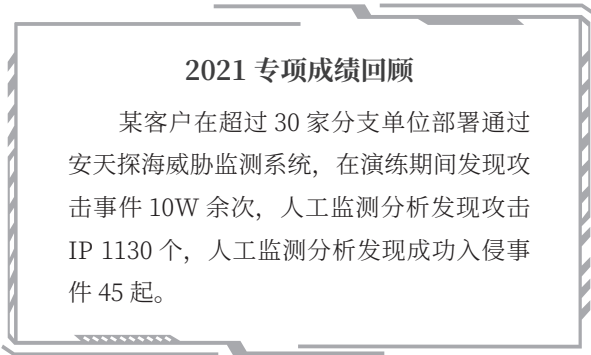
1.5 网络边界监测



图5 网络边界监测服务

演练前，收集网内对外开放服务的资产列表、域名列表，部署安天探海威胁检测系统，对网络边界流量进行深度分析，建立流量安全基线。

演练期间，通过安天探海威胁检测设备发现网络扫描、漏洞利用、异常流量、恶意文件等攻击事件，并协助追溯攻击，先后形成威胁情报表单、详细分析报告，



协同封堵恶意IP，同步被入侵情报信息给现场服务人员，开展取证分析，上报演练指挥部，获得加分。

演练结束后，全面总结网络边界监测服务工作成果，输出《网络边界监测总结报告》。

1.6 终端威胁检查

演练前，为用户网内所有主机部署安装安天智甲终端防御系统，通过管理中心实现终端安全一体化管理，帮助管理人员了解网内终端安全情况，查看安全事件详情；同时，通过智甲管理中心下发指令统一对网内所有主机进行威胁排查，排查潜伏在主机上的木马病毒。

演练期间，借助智甲管理中心进行实时安全监测，及时发现并处置在演练期间内网主机新出现的木马病毒。

演练结束后，全面总结终端威胁检查服务工作成果，输出《终端威胁检查总结报告》。

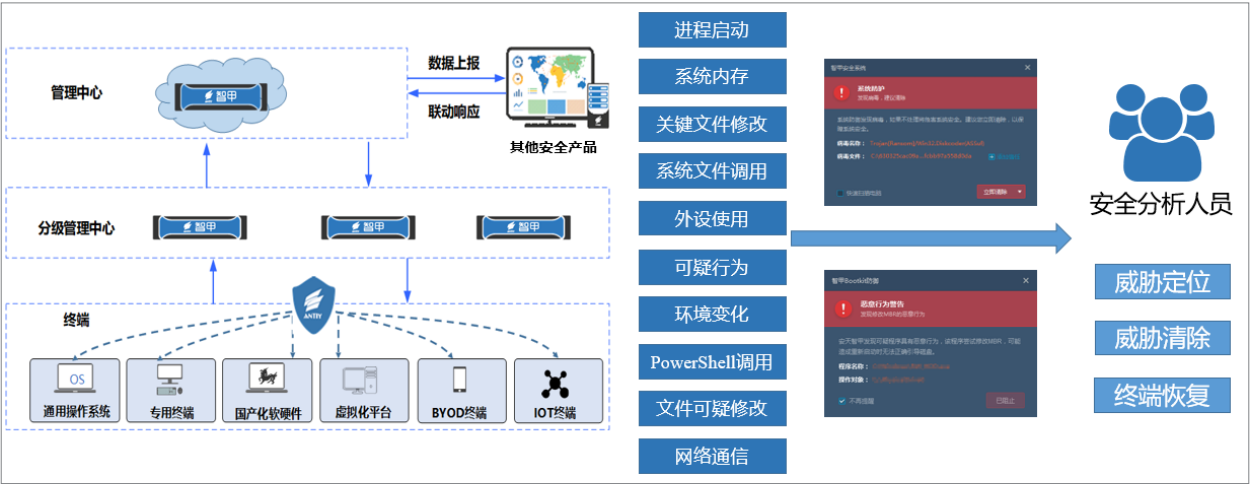
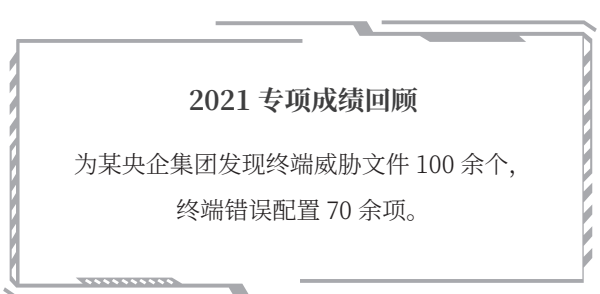


图6 终端威胁检查服务

1.7 欺骗式防御

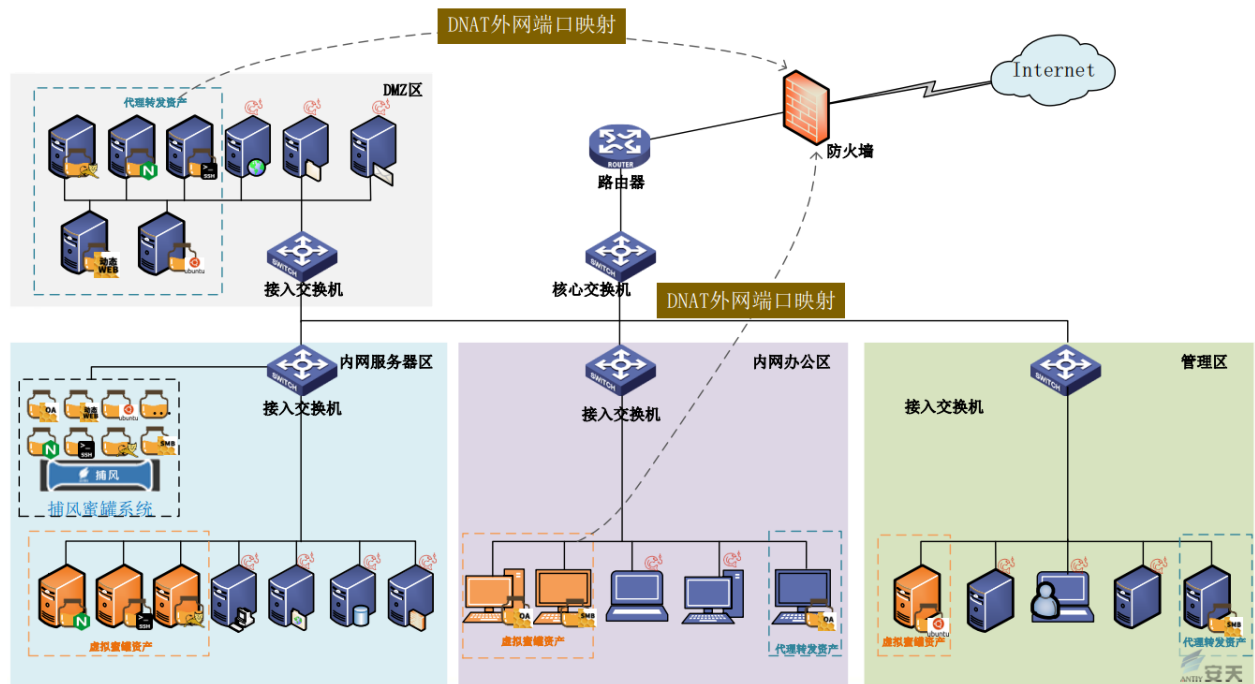


图 7 欺骗式防御服务

安天威胁诱捕分析服务基于安天自主研发的捕风蜜罐系统开展，通过构建欺骗式防御手段，诱使攻击方攻击，分散攻击方注意力的同时，使攻击者暴露攻击行为、攻击意图，进而保护真正资产安全。安全工程师将实时排查蜜罐日志与告警，确认用户网络存在的威胁载荷、失陷主机、攻击方作业手法，处置发现的安全事件，提供网络加固建议，优化网络防御能力。

演练结束后，全面总结欺骗式防御服务的工作成果，输出《欺骗式防御总结报告》。

2021 专项成绩回顾

为某客户单位内网靶标系统所在的网段部署蜜罐，监测发现多起针对靶标系统的攻击探测行为，并及时协助客户调整防守策略，成功阻断攻击事件，进一步分析溯源累计加分 900 分。

2. 案例：有效帮助客户不丢分并多加分

安天针对攻防演练防守要点，结合自主安全产品，通过覆盖网络攻防演练全生命周期的解决方案与深入场景化的专项防护，为客户构筑的动态综合的防御体系，真正实现了动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的全场景赋能安全防护效果，为演练活动的组织和防护提供有力保障。有效帮助了客户不丢分并多加分。



图 8 安天攻防演练服务获得的部分客户感谢信

案例一：某能源集团攻防演练防守保障

安天为某能源集团总部及其二级单位、电站电厂提供整体攻防演练保障服务，通过部署安天态势感知系统、安天探海威胁检测系统、安天智甲终端防御系统，结合演练前风险排查和演练期间 7*24 小时监测值守服务，共计监测到威胁告警 2 万余次，整个演练期间，内网区和工控区均未发生攻击成功的安全事件，整个演练期间该集团零扣分。

案例二：某运营商攻防演练防守保障

安天为某运营商总部提供整体安全保障服务，通过演练前的资产梳理、安全排查与加固，演练期间进行

7*24 小时监测值守，共计监测到威胁告警 5 万余次，为其发现并处置多个 0day 攻击事件，整个演练期间该运营商零扣分。

案例三：某央企攻防演练防守保障

安天为某粮油食品行业的央企集团提供整体防护保障服务，协助其进行整体防御部署，通过部署安天的探海威胁检测系统、智甲终端防御系统、捕风蜜罐系统、追影威胁分析系统等，结合演练前风险排查和演练期间 7*24 小时监测值守服务，共计监测到威胁告警 3 万余次，并对多起攻击事件进行溯源分析，累计加分 1000 余分。

终端 / 云主机安全防护

承载各类业务的服务器和主机一直是网络威胁攻击（包括各类攻防演练）的跳板和最终目标。在攻防演练活动期间，当攻击者突破外层防护后，往往就比较容易实现横向移动、跨域攻击，所以终端就成为了防护最后的堡垒。

1. 终端侧防御

智甲终端防御系统（以下简称：智甲）在企业网络

信息系统环境中可提供全周期、实时的主机资产监控与加固、异常事件分析、威胁处置、运行管控等多种能力。

在攻防演练准备期，智甲可作为资产风险检测系统，通过对资产的脆弱性、暴露面的检测，发现资产存在的安全风险，并提供处置方案，提高资产威胁防护能力；

在攻防演练活动间，智甲可提供环境锁定功能，通过白名单管控、访问管控等严格管控手段，拦截各类网

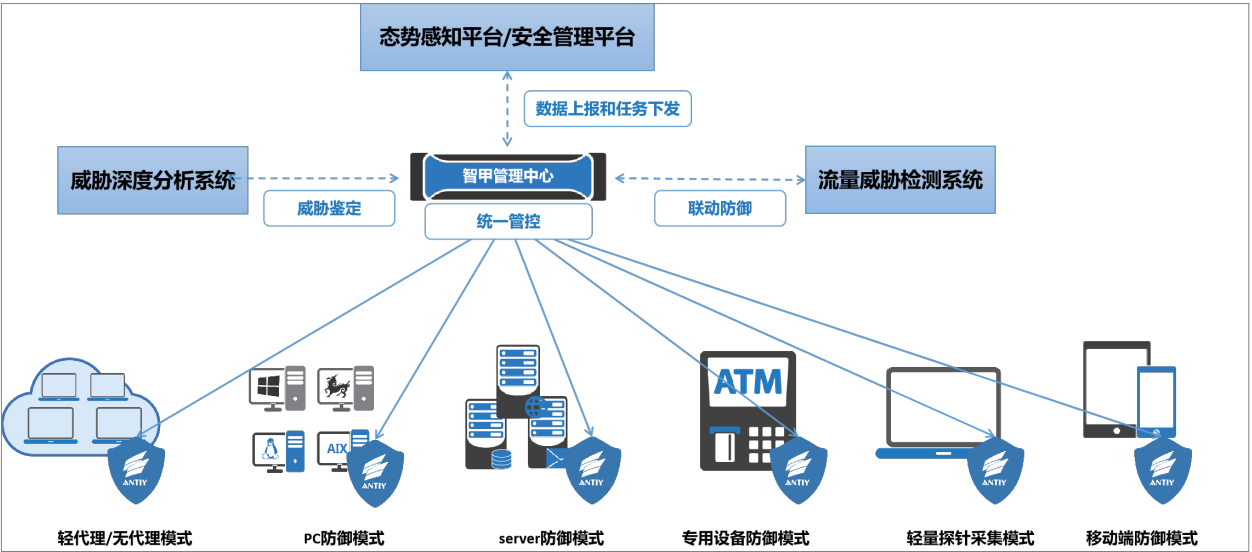


图 1 智甲可适配丰富的应用场景

络攻击，支撑快速响应与处置任务，充分保障主机内系统与数据的安全。

丰富的应用场景适配可满足用户在演练与日常安全防护中端点侧多样化威胁防护的需求。管理中心可实现对各种端点类资产进行统一安全管理，集中监测分析端点安全事件、制定和下发相关处置任务策略，降低安全运营工作量，提高工作效率。

1.1 七项产品价值满足演练场景需求

支持为多平台、多场景提供安全防护能力，可应对演练期间防守方不同场景需求，并实现统一化管理；

演练前全面清理企业内网僵尸蠕毒以及黑客工具等隐患，降低在演练过程中被打穿风险，有效避免防守人员在演练期间误判告警事件；

演练期间实时防护终端，根据防护策略自动处置、清除 / 隔离恶意文件，或阻断程序 / 终端联网行为等；

协助防守方安全人员对攻击进行快速排查、定位、全网追溯，评估影响范围，威胁文件一键全网清除；

联动其他安全设备，如与安天追影威胁分析系统和安天探海威胁检测系统联动，对发现的各类威胁协同处置，快速响应；

演练期间可作为终端代理，为统一安全运营中心提供各类终端日志和告警信息，为攻击的关联分析、追踪溯源提供完善数据；

良好的运维管理能力与集成能力，威胁查杀、进程防护、漏洞检测、虚拟补丁、终端管理、网络防护一体化，一机部署解决多种问题。

2. 云主机侧防御

安天智甲云主机安全系统（以下简称：智甲云主机）是安天自主研发的面向多云、混合云的云主机安全系列产品，用于帮助用户建设以资产安全为核心、风险防范为重点、安全事件为驱动的统一云安全运营管理体系。

智甲云主机能够有效提升主机和容器的安全预警、检测、防护、响应能力，使用全生命周期管理机制进行持续跟踪，赋予安全数据以空间、时间、状态属性，与实际网络环境关联整合，对安全数据进行全面分析，通过安全数据详细分析与过滤，快速识别高风险、有价值安全问题，为安全决策提供依据。

2.1 产品攻防演练价值

智甲云主机安全系统可以提供资产清点、风险发现、威胁检测、容器安全、微隔离、合规基线检查、威胁情报、威胁猎杀能力。产品各项功能数据互通，相互联动，能够为用户提供一站式云安全防护，全面提升云安全建设水平。

提供混合数据中心架构下统一的安全管理能力，适应用户多云、混合云等各类复杂 IT 环境，并可根据实际情况将产品功能、配套服务按需灵活搭配，能够让用户对所有云端资产、合规状况一目了然，同时可以协助用户对云主机进行实时监控，了解其安全状态。

一站式获取资产清点、风险发现、威胁检测、微隔离和容器安全等安全能力，精准检测外部威胁、内部风险，防护云中资产安全。

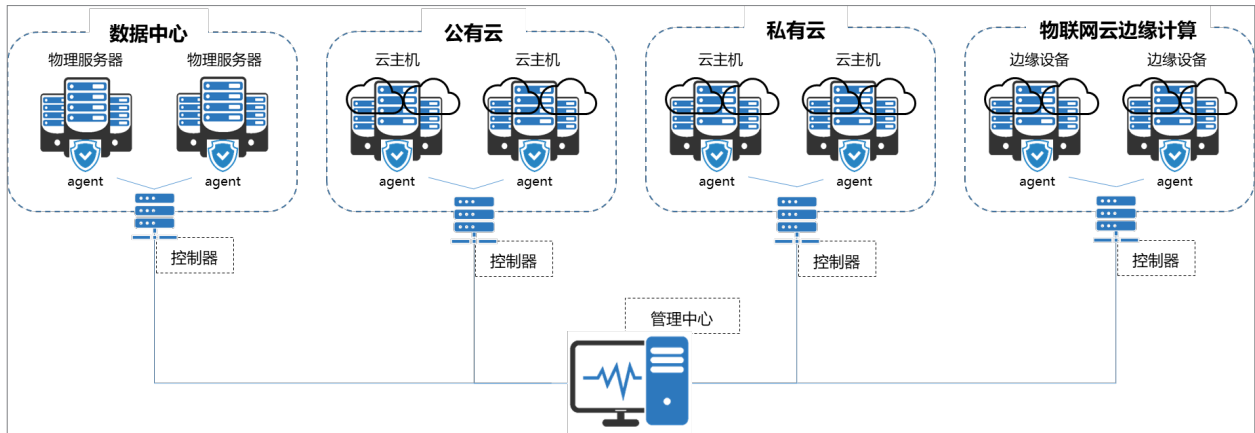


图 2 智甲云主机部署示意

流量侧持续监测

无论是在攻防演练期间还是在日常状态下，利用网络资源发动攻击，都是攻击者优先选择的手段。承载网络信息连接流转的流量侧，既成为了攻防对抗的第一条“战线”，也是防守方的第一道“防线”。

所以，持续有效的流量侧监测与及时的联动处置，在一定场景下，就成为了防守方在攻防演练实战对抗中“速战速捷”，获得主动的“关键”。

依托安天 20 余年对网络威胁行为体的持续跟踪及威胁对抗经验、以及多年大型攻防演练防守保障经验的积淀，安天探海威胁检测系统（以下简称：探海）以增强用户在真实威胁对抗中的分析、检测、处置、协同能力为核心，可快速发现威胁并及时响应，提升整体网络安全保障能力和防护水平。

在攻防演练场景中，通过在网络关键节点旁路部署探海，可在演练备战阶段，检测网内被植入的恶意代码，清除潜伏木马；同时也能在演练期间，实时监测网络威胁与攻击行为，并协同联动其他安全产品及时处置；进而有效帮助用户在演练期间，固守网络侧安全，保障少丢分或不丢分。

探海的全要素记录机制，可提升对定向攻击、高级威胁的检测响应和溯源能力，能帮助用户定位攻击感染源头，并持续感知网络攻击、监控攻击者的各种行为，同时可辅助安全分析人员有效溯源攻击过程，快速高效完成溯源分析总结报告；支撑在演练期间争取多得分。

1. 四项产品价值，满足演练场景需求

1.1 威胁检测及实时告警

探海内置恶意代码检测引擎、网络行为检测引擎、命令与控制通道检测引擎、自定义场景检测引擎等四大检测引擎，采用 DGA 随机域名检测、隐蔽信道检测等多种威胁检测模型，支持从数据流、网络行为、文件等多个层次对采集的数据进行检测，发现处于不同攻击阶段

的威胁活动，及时监测扫描探测、钓鱼邮件、漏洞利用等攻防演练中常用的攻击手段，识别攻击路径。并通过界面提示、设备联动、邮件等方式，对捕获的威胁事件实时告警。

1.2 自动化事件关联分析

探海基于载荷相似性、恶意代码家族关联性、攻击资源相关性、漏洞相关性、威胁情报关系、攻击活动上下文、时序关系等维度，对发生在一定时间窗内的多条威胁事件进行统一的自动关联处理，对演练期间攻击方的扫描探测活动、载荷投放、命令控制通道的建立、木马的通联活动与回传行为进行统一监控，并生成详细的分析报告。同时，还可通过还原攻击过程，提高安全分析人员的工作效率，帮助用户及时进行威胁处置。

1.3 资产风险可视化评估

在演练期间，面对流量中发生的网络威胁，探海可提供高危资产画像信息，帮助安全分析人员快速直观地看到 IP 基本信息、通联关系、域名使用情况、源端口使用情况、监听端口开放情况、攻击详情等信息，协助用户还原威胁事件全貌，洞见内部网络威胁，为关键资产制定针对性策略提供数据支撑。

1.4 关键数据按需采集

针对演练期间发现的网络威胁事件，探海支持 IP、协议或端口进行全流量捕获和全包存储，可根据演练场景进行流量捕获策略的配置，为后续的追踪溯源、分析研判提供有效支撑，提高应对威胁分析响应速度。

2. 四大能力优势，支撑实战化运营

2.1 多层次多维度检测，网络威胁有效发现

探海支持从数据流、网络行为、文件等多个层次对网络威胁进行检测，综合运用恶意代码检测、行为检测、威胁情报、模型分析、关联分析等多种检测手段，对演练期间处于不同攻击阶段的网络活动进行精准检测与

告警：包括但不限于网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动等网络攻击行为；以及发现 DGA 随机域名、隐蔽信道等新型网络攻击行为。实现快速并精准地发现演练中的网络攻击行为。

2.3 多产品协同联动，网络威胁及时处置

探海与安天追影威胁分析系统联动进行深度分析，弥补传统边界设备和入侵检测设备检测深度不足的缺点，及时检测虚拟化 / 沙箱逃逸、漏洞规避防御等恶意行为，



图 1 探海多层次多维度检测示意

2.2 全要素留存，网络威胁有效分析

基于流量侧海量的威胁线索，如何做到有效溯源分析，是网络安全检测重要的一环。区别于全流量缓存记录的方式，探海基于流量侧的细粒度协议解析和还原，支持对网络元数据、应用层传输要素、载荷对象要素等要素信息进行全要素留存，为演练期间的网络攻击溯源提供更精准、更全面的威胁线索，同时基于恶意代码传播关系、命令与控制关系、恶意文件关联等维度，进行网络侧威胁事件自动化关联分析。

同时，依托安天 20 余年网空威胁研究与对抗经验，借助 ATT&CK 威胁框架，结合威胁情报上下文进行自动化多维关联分析，能更有效地支撑安全分析人员进行威胁研判、追踪溯源，显著提高网络攻击分析效率。

特别是 0day 漏洞攻击等高级攻击技术手段。同时，探海也可以与安天智甲终端防御系统联动，协助威胁处置，形成安全运营闭环。

2.4 场景化规则能力，构建攻击者难以预知的检测策略

在演练期间，虽然攻击方的攻击手段多样化，但探海支持通过持续将人的经验转化为适合用户私有场景的自定义检测规则，从而构建攻击方无法预知的检测防御策略，形成攻防场景下私有化、定制化的威胁对抗能力，提升对纵深威胁的检测能力。

运用文件分析提升威胁发现

当前的网络攻击手段呈现出组织化、规模化、复杂化的特点，但无论是普通威胁亦或是高级持续威胁，在“载荷投递”与“命令与控制”阶段（出自 cyber-kill-chain）均大概率会将攻击手段以落地文件的方式投递到目标系统当中，因此在面对网络攻击时，对攻击过程相关文件分析一般都能够发现攻击者的意图，协助防守者对症下药进行更有效的防御。

在攻防演练中，投递未知载荷（或者投递针对性免杀载荷）可能躲过规则检测，使用“文件行为系统”发现文件本身的恶意行为将是破局的重要手段。

1. 演练场景需要“快准深”兼具的文件分析产品支撑

目前市场上传统的文件分析方式主要有两种：杀毒软件与沙箱分析（防火墙中的防病毒模块、防病毒网关等设备一般也是将流量中还原文件进行杀毒软件扫描判断是否恶意）。杀毒软件主要依赖库文件进行扫描匹配，优势在于检测速度快、误报率低，适合文件量大，需要快速出结果的场景。沙箱分析的优势则在于不依赖于库文件，能够对文件的真实行为进行识别判定，但分析效率不高。所以，以上任一的文件分析方式，都不能全面满足在攻防演练场景中，需要快速、精准、深度的完成文件分析现实需求。

安天追影威胁分析系统（以下简称：追影）作为高级威胁发现的手段之一，融合了上述两种分析方式的特点，依托全球领先的安天下一代威胁检测引擎，核心技术自主可控，可以确保为用户提供及时的威胁分析响应速度，并降低外部技术依赖风险。

同时，追影也汲取了安天十余年积累的自动化分析经验，在内置安天下一代威胁检测引擎与动态分析引擎的基础上，还集成了十余种分析模块，包括黑白名单模块、文件来源检测模块、元数据提取模块、数字证书提取模块、

webshell 检测引擎模块、潜在能力分析引擎模块、情报交换引擎模块等，可有效实现对文件进行多维度分析鉴定。

对于高对抗性的恶意文件，追影动态分析环境支持 Windows 和 Linux 等主流操作系统及 Office、Adobe、Firefox 等常见的应用软件，全面构建符合用户实际使用场景的分析环境，即使面对定向攻击时也能识别未知文件的恶意行为。与此同时，还可进行用户操作模拟、网络模拟、移动介质高仿真模拟等，以应对样本的各种触发条件；并可有效发现与对抗反分析行为，降低分析漏报率。

此外，针对某些需要在特定的环境下才能够触发相应行为的恶意文件，追影支持人工干预动态分析过程，调整样本在虚拟机中的运行条件、运行环境，最大程度地触发样本行为；并提供样本在不同虚拟环境中的行为对比，揭示样本的环境偏好。

追影不但能够将在动静态分析过程中，提取的静态特征和动态行为相结合，依据文件的特征相似、行为相似、内容相似及文件间的衍生关系，鉴定并分析各类已知与未知威胁，有效检测未知漏洞利用、免杀木马、商业军火、APT 组织的专用木马等高级威胁，提升用户的高级威胁对抗能力；还能通过情报交换组件的情报发布与消费能力与追影内部情报生产能力相结合，为用户生产私有化情报，在演练活动中能够将追影的能力有效传递至各个产品，提升整体威胁发现的能力。

2. 四项能力有效提升演练场景整体威胁发现能力

2.1 海量样本及时判定

追影具有高性能的动静态分析能力，静态分析每天可以分析超过 25 万的文件，动态分析每天可以分析超过 3 万的文件，并能够通过多台追影组建集群的方式对性能进行快速扩展，能够帮助用户对演练活动中捕获的海

量样本文件进行及时有效的分析和判定，出具详细的报告，及时发现可疑文件，供安全分析工程师进行追踪研判。

2.2 为其他安全设备提供执行依据

追影威胁分析系统能够与安天其他安全产品深度结合，形成发现、响应、处置的防御闭环；此外，追影也提供完整的上传、下载 API 接口，对其他产品进行安全赋能，为处置类产品提供根本的执行依据，提升整体方案的防御深度和准确性。

2.3 手动干预分析过程，提升演练场景的贴合度

追影提供的手动干预样本分析过程的能力，可对特定类型的文件进行手动指定运行参数的能力，保证样本在沙箱环境中能够真实触发。此外，追影也能通过添加

AUTOIT 脚本的方式模拟用户对系统的直接操作，提高环境的仿真程度，最大限度提升环境与演练场景的贴合程度，从而及时发现针对演练场景的威胁样本，提升整体威胁检出能力。

2.4 支撑私有化情报生产能力

追影能将样本文件进行细粒度的向量拆解，并将拆解出的向量进行情报化处理，通过内置的情报交换组件进行情报生产与消费。可在演练活动中迅速将单点情报同步给整体情报网，提升整体安全防御的敏捷性，能够实现将出现过的威胁迅速同步给其他安全设备，保证整体情报的时效性与可靠性。

及安全措施信息，为攻击决策提供支撑。

第二阶段：建立据点

通过分析漏洞，发起定向攻击，同时也会对目标现有安全措施进行突破。此阶段的主要目标是：确保通过攻击获得对应用程序或底层系统的访问权限之后，仍然可以保持持续的访问状态。因为，只要能够维持对系统长期有效的访问权限，就能更深、更远地接触到其他相关应用，从而获取更多的信息。

第三阶段：横向移动

通过在被攻陷的目标内网进行横向移动，尽可能的获得更多权限；同时，对目标进行内网情报收集，主要包括当前主机情报与内网扫描探测情报。

针对上述攻击链条与思路，可在互联网部署 ERP、OA、VPN 系统、虚拟化桌面系统、邮件服务系统等高交互蜜罐资产，并且选择部分蜜罐资产预置不同的弱口令、漏洞等诱骗攻击者；同时散播虚假信息“蜜饵”，干扰攻击者收集情报，使其选择攻击目标时产生误判，指数级地增加攻击者的攻击成本，延缓攻击进程的同时，将

攻击者不断诱导引入蜜罐陷阱，从而诱捕攻击者，保护真实资产。



图 1 攻击方的进攻思路

2. 安天捕风蜜罐系统部署策略与演练价值

2.1 战前准备，构建阵地

资产梳理

基于企业自身资产管理积累，结合安全技术支持，对企业互联网、内网资产进行全面收集，主要涉及资产类型包括：主机资产、域名资产、Web 应用资产、GitHub、网盘等互联网敏感信息泄漏等，并对测绘结果进行确认，责任到人。在不影响业务的前提下，尽可能收缩资产暴露面，加强资产可控性。

在必要路径部署安天捕风蜜罐产品

分别在内外网部署多套安天捕风蜜罐系统对攻击者进行诱捕。

互联网区域资产以 Web 资产为主，根据攻击者情报收集的特性，在互联网侧部署大量高交互 Web 蜜罐，诱导攻击者对蜜罐系统进行攻击。为提高迷惑性，此类蜜罐均克隆自企业真实的业务系统，例如：邮箱系统、网

盘系统等等。攻击者一旦对上述蜜罐发起攻击，蜜罐管理端即可监控到攻击者的源 IP、攻击手法、时间等信息，蜜罐内置信息获取脚本，可读取攻击者浏览器缓存的社交账号信息，通过这些信息可开展溯源反制相关工作。针对内网，攻击者通常会先对各网段进行探测，尝试对暴露的端口服务进行攻击，根据这一特性，内网部署大量服务型蜜罐，用于迷惑攻击者，增加攻击发现概率。

防护、监控类设备关键节点部署

面对互联网庞大的攻击流量，全量监测实现难度高、代价大，自动化攻击阻断、流量清洗是一种不错的手段。在各网络边界均部署防火墙，设置端口级访问控制策略，对互联网流量实现初步过滤；防火墙后依次部署 IPS、WAF 等阻断类设备对流量进行规则匹配，阻断其中绝大多数攻击流量；同时，在各个安全域部署流量分析蜜罐探针，对流量中的攻击行为进行分析，如此层层过滤，实现攻击流量全方位监控。

2.2 提前布局，以逸待劳

针对攻击路径布局安天捕风蜜罐的诱饵和探针，包括外部攻击欺骗、内部环境大量部署、外联欺骗等多个攻击方向的欺骗布局，尽可能多的对攻击进行欺骗，获取其攻击数据，从而检测潜在的未知威胁，为新的本地化威胁情报提取提供基础的威胁事件信息和充足的原始数据信息。

并利用网络中的空闲的资源，感知新的攻击趋势和威胁。包括空闲的端口资源，联动安天智甲用终端空闲端口转发给蜜罐、安天镇关防火墙的映射出外网，以及针对数据中心私有云混合环境的云内探针联动，都可以较好的扩展覆盖面增加感知面。

捕风蜜罐的自动构建资产技术，可以通过对真实网络环境资产探测学习，充分利用空闲 IP 资源自动构建与真实环境相似的、具备深度交互多层次仿真的伪装蜜罐网络。同时，能够判断真实资产配置 IP 与自动创建伪装资产 IP 是否冲突，并支持跨 VLAN 的环境下的自动海量蜜罐资产的伪装，达到自动、智能、大量构建伪装资产的能力，大量的自动伪装蜜罐在网络内部更加容易感知网络内部的横向移动行为，同时使攻击者难以区分真实

资产和伪装资产，无法快速命中目标。

捕风蜜罐支持自定义资产模板组合，可自由组合将已有的模板组合成新资产模板，同时可以利用空闲主机作为代理节点来动态扩容蜜罐仿真、感知范围，以此达到蜜罐服务的灵活暴露以及更高数量级的蜜罐服务数量，从而实现迷惑攻击对手保护真实资产的目的。

有效降低攻击者通过内部横向扩散带来的风险。捕风蜜罐的蜜罐网关外联欺骗能力，既可以误导攻击者，也可以利用该特性发现内部已失陷主机。同时，可与防火墙联动，对威胁情报检出的攻击 IP 进行拦截。

2.4 诱敌深入，请君入瓮

捕风蜜罐可以通过在蜜罐资产中投放虚假数据制作

常用仿真服务列表		
蜜罐类型	特点	溯源能力
应用服务蜜罐	支持伪装 CRM、信呼 OA、Nginx 等常见系统，可以自定义预置用户名密码，具备一定的交互能力。	IP 信息、社交账号、攻击喜好、媒体信息。
系统服务蜜罐	支持伪装 OpenSSL、Windows 7 等常见系统，可以自定义预置用户名密码，具备一定的交互能力。	IP 信息、社交账号、攻击喜好、媒体信息。
数据库蜜罐	支持伪装 MySQL、MongoDB、Oracle 等常见系统，可以自定义预置用户名密码，具备一定的交互能力。	IP 信息，植入 URL 等。反制数据库请求等。
网络设备仿真蜜罐	支持伪装华为路由器，防火墙等常见系统，可以自定义预置用户名密码，具备一定的交互能力。	DNS 劫持等捕获劫持域名站点。
工控设备仿真蜜罐	支持伪装 IPMI、BACnet 等常见系统，具备简单的交互能力。	攻击 IP、漏洞植入下载 URL 等。

2.3 监控分析，知己知彼

捕风蜜罐采集包括网络数据、系统日志、应用日志、文件等数据。

通过全面采集可以提高某些攻击行为的检测可能性，比如针对 SSH 的暴力破解行为，并可以记录黑客尝试的不同账户密码信息。

同时，对采集到的数据进行对应分析与展示。分析包括但不限于：攻击时间、攻击行为、攻击阶段、攻击方式、威胁等级、受攻击资产等；结合攻击数据（如 IP 地址、网络、URL、攻击样本等）生成可视化图表，用以支持对攻击事件的逻辑复现及攻击行为全过程分析，进而发现攻击者目的、目标、手法、技术等。并可生成对应的攻击情报数据，充实数据情报库并用以展现使用。

捕风蜜罐通过以上维度对蜜罐资产进行实时监测，可以识别出扫描、漏洞入侵、Webshell 植入、黑客工具植入等 50 多种威胁行为，并具备防止攻击逃逸的能力，

的蜜饵文件、反制 VPN 程序，可通过进一步提升甜度使得攻击者产生已经攻入真实系统的错觉，同时获取更多的攻击者的信息，甚至进一步反制攻击者。

在攻击者攻击进入蜜罐仿真系统内部对外连接通信时，蜜罐网关对蜜罐内部请求流量进行欺骗应答，从而进一步激发攻击的网络或系统行为。可以针对网络请求，如 DNS 请求、TCP 请求、URL 请求、Ping 等进行响应及交互等欺骗应答响应，在保障内外资产安全的情况下，激发出更多流量进行蜜网流量检测模块的威胁检测。

2.5 情报生产，快速普查

捕风蜜罐在监测的安全事件中提取攻击者投放的文件哈希、网络恶意域名、C&C 等情报特征，经过海量文件、域名、IP 白名单过滤，形成可协同监测的本地化威胁情报。

监测方式主要采用静态解密和动态分析提取样本文件的网络信标。针对样本识别、网络信息提取并经过白域名 IP 过滤后产生网络威胁情报，提取攻击源 IP、样本

MD5、C&C 提取等。由于攻击者或者恶意程序的威胁活动中涉及的网络、文件等操作很多包括正常的站点，比如百度、微软等域名站点测试联通性，释放一些辅助的语言程序包文件等。因此本地化威胁情报生产需要安全厂商提供高质量的白名单进行过滤，针对安全事件中提取的指标进行误报排除。白名单需要持续地从各个操作系统、补丁跟踪、应用程序发布站点获取建立广泛的白名单库。网络白名单则需要建立各个类型的信任站点持续跟踪相关的资源变化。

2.6 溯源分析，擒贼擒王

安天捕风蜜罐系统使用基于 JSONP 跨域获取信息的网络溯源方法，通过跨域技术调用相关社交媒体账号的接口，穿透代理，实现跨域资源获取，从而实现抓取攻击者社交 ID 的功能。

捕风蜜罐系统支持识别攻击者的网络身份（网络 ID、手机号、用户名、邮箱等）、设备指纹、使用的操作系统等，支持识别苏宁、搜狐、yy 语音、雪球网、爱奇艺等网络 ID。

在一系列的诱捕，情报收集后，已基本完成攻击者的信息采集，从而对攻击者进行画像、追踪和溯源。

通过基本信息溯源：IP、位置信息

传统的基于 IP 的溯源法对攻击者的身份信息获取很有限，很难及时进行有效溯源和反制。蜜罐系统则给了防守方反制的机会，通过蜜罐预设的反制段，主动获取攻击者主机或者网络信息，捕风蜜罐系统可以对某个 IP 进行多维度的信息查询，通过关联人员、地址、注册单位、邮件、域名关键字等信息，可对攻击 IP 进行画像，进而参考社交信息溯源进一步管理分析，可将攻击者定位至自然人、单位组织。从而更准确的定位攻击者的身份，实现更精准的溯源。

通过社交信息溯源：微信、QQ、手机、邮箱等

1) 利用通信平台，添加好友，套取信息；
2) 利用其注册昵称，查询在其他站点同名注册者；
3) 对比社工库信息，进一步锁定攻击者信息。最后将各平台获取的信息整合，完整拼凑出自然人画像。安天捕风蜜罐不仅具有优秀的威胁捕获能力和溯源能力，在安全运营中，同样可以扮演增强企业安全防护建设能力的角色，为构建安全网络世界做出重要的贡献。



图 2 攻击者画像分析绘制示意

WEB 在线实时主动防御

Web 应用防火墙（Web Application Firewall，简称：WAF）通常部署于 Web 网站前端，为目标网站提供在线实时的安全防护。WAF 对网站的 HTTP 流量进行解析，基于解析结果进行深度 Web 攻击扫描，检查流量数据中是否包含 XSS、SQL 注入、已知漏洞等相关 Web 攻击特征，对触发安全策略的流量进行实时的告警和阻断。

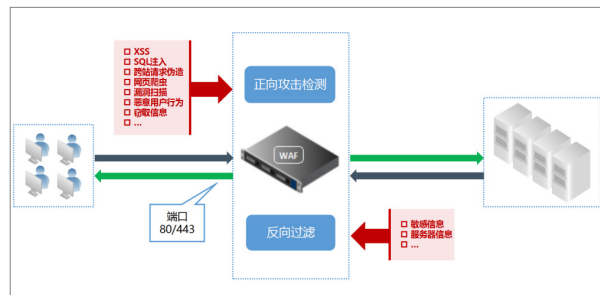


图 1 Web 应用防火墙作用示意

WAF 在攻防演练中是一款不可或缺的 Web 安全防护设备，是保护 Web 服务器最重要的一道安全门。安天下一代 WAF 防护系统以积极防御为安全理念，一改传统 WAF 以特征匹配为中心的设计思路，从用户自身的网站安全出发，通过对网站关键业务、数据进行动态变形、封装，结合网站代码反调试保护和客户端环境实时主动探测技术，以我为主对网站进行主动防护，能帮助用户在演练期间化被动为主动。

安天下一代 WAF 防护系统的四大产品价值，可有效支撑用户摆脱传统 WAF 在攻防演练中被动挨打的局面。

1. 价值一：增强的传统 WAF 安全功能

1.1 强化的攻击特征检测技术

高速特征关键字预匹配技术保证在超大流量下实现对特征的全面检测；特征关联匹配技术提供强大的特征描述能力，支持对复杂行为特征进行定义；完善的 Web 递归解码引擎，有效应对攻防演练中的各种攻击检测规避技术。

1.2 全方位的 WebShell 检测手段

产品从上传文件、RFI（Remote File Inclusion）攻击防护、WebShell 指纹检测、基于访问授权的 WebShell 检测等多个环节全方位检测 WebShell，可有效防止网站在演练期间遭受挂马攻击。

1.3 API 安全防护

通过 API 传输的数据类型通常为 JSON 或 XML 格式。产品针对该格式数据进行专门的解析，并基于解析的结果对数据格式与元素进行规范性检查和攻击特征检查。确保攻防演练过程中网站对外的 API 服务安全。

1.4 客户端运行环境安全加固

从近年攻防演练趋势来看，攻击方越来越多地通过攻击客户端来间接完成最终对目标网站的渗透。客户端浏览器安全功能通过插入相关浏览器安全属性对客户端进行安全加固，弥补用户网络安全环境短板，将 WAF 的安全防护能力延展到 Web 客户端，从而提升用户 Web 应用链的整体安全性。

1.5 强大、灵活的安全策略定制

产品允许用户关联多种 HTTP 元素和变量来定义具有复杂逻辑的复合安全策略，应对演练期间不同场景下的安全需求，有效避免产品的定制开发。具体的产品支持的元素和变量包括 URL、参数、HTTP 头部字段、请求资源类型、HTTP 返回码、来源 IP、客户端地理位置、用户名、时间范围、触发频度等。

1.6 网页防篡改

网页防篡改功能能够锁定被保护的网站页面，即使发生目标网站页面被攻击者篡改情况，依然能向用户提供正常的页面服务。网页防篡改在攻防演练中能够起到亡羊补牢的作用，最大限度消除网站漏洞带来的负面影响。

1.7 丰富的 HTTP 访问控制方式

产品提供 IP 黑名单、Geo 访问控制、URL 访问控制、

Host 访问控制等多种 HTTP 访问控制方式。在演练中能对攻击来源进行高效的封堵。同时对外提供 RESTFul API 接口，实现与其它安全类产品的联查、联防。

2. 价值二：自学习快速创建安全策略、防御 0day 攻击

自学习功能能够自动分析、学习目标网站的流量，如网站拓扑结构、参数详细信息、常用 HTTP 方法以及特征误报等。通过自学习，产品可以快速地生成拟合目标网站的配置，极大地缩短了演练前期 WAF 部署、调试的周期，并大大提高了配置定义的准确度，规避了人工创建安全策略存在的弊端。

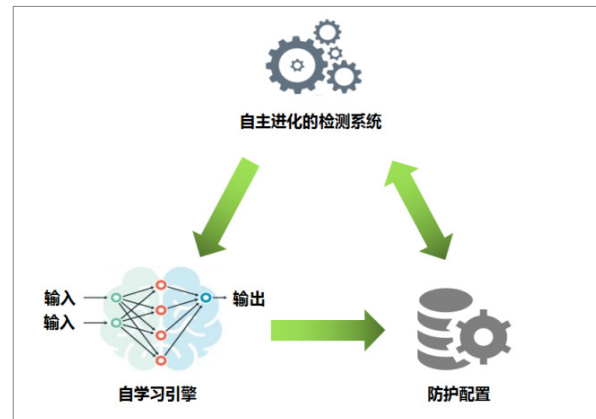


图 2 安天下一代 WAF 防护系统自学习逻辑

自学习通过关联“特征检测”可以在演练期间帮助用户自动处理误报，将用户从繁杂的误报处理工作中解放出来，着重应对、处理更为关键的安全问题。自学习经过对网站流量分析与统计，能够学习业务参数的相关细节，并为业务参数创建基于白名单的规范策略。这种白名单机制的参数规范策略可以有效地应对 0day 攻击，阻断带有不符合预期参数规范的 HTTP 请求，使得攻击者无法通过构造参数的内容来利用 0day 漏洞。

3. 价值三：综合的自动化攻击防御方案

针对近年来攻防演练中不断增多的 AI 和自动化相关工具的使用，产品从用户业务安全加固、关键资源防护、业务代码保护、客户端环境主动探测及验证等多个维度

提供综合的自动化攻击防护解决方案。

3.1 对用户关键业务进行安全加固

产品可以对用户业务的各个环节进行安全加固，如注册、登录、查询、下单等业务环节，有效地防范攻击者利用自动化工具进行虚假业务交易、薅羊毛、账号撞库等活动。通过对用户业务的安全加固增加了自动化工具的攻击难度和成本，使得自动化工具无法简单、直接地攻击用户的业务，攻击者无法直接控制和构造业务参数和访问令牌。

3.2 对网站业务资源的专门防护

产品通过对用户业务 URL 进行加密、添加一次性访问 Token、HTML 链接元素动态变形等技术对用户的关键业务资源提供专门的防护，有效防止用户业务资源被数据爬虫窃取。

3.3 客户端环境主动探测

产品通过在网站回应的页面中插入环境探测脚本，对页面最终运行的客户端环境进行采样、探测，搜集客户端环境的各种参数和用户事件，如浏览器版本、客户端类型、用户的键盘、鼠标事件等，综合评判客户端是否是真实的浏览器环境。

3.4 自动化工具被动检测

产品具有机器人被动探测机制，通过在服务器回应的页面中插入机器人诱饵，诱使机器人访问，检测恶意机器人客户端。

3.5 用户业务代码反调试防护

产品具有用户代码反调试防护能力，通过在用户的代码中插入反调试干扰指令，使得攻击方无法对被保护的代码进行跟踪、调试。这种方式在演练期间增加了攻击方的攻击成本，保护网站的代码逻辑不被攻击方所破解。

3.6 灵活、多样的人机验证方式

产品提供脚本挑战和验证码的人机验证方式。对于普通的自动化工具，由于其不是真实的浏览器，无法成功运行产品的挑战脚本，无法通过验证。这种脚本挑战方式优点在于其过程对于终端用户完全透明，不会影响用户体验。

对于使用浏览器引擎（无头浏览器）开发的高级自动化工具，通过验证码方式可以对其进行识别。该方式的优点在于即使安全策略出现误报，只要用户在输入正确的验证码后依然能正常访问网站业务。

4. 价值四：用户业务安全防护

用户业务安全防护功能能够抵御攻防演练中针对用户业务层面的攻击。

4.1 用户识别与跟踪

监控网站用户的登录过程，对用户身份进行识别，将业务流量映射到具体的用户。在用户识别的基础上，进一步跟踪用户的业务操作。对于用户触发的所有安全策略告警，产品都能对应到具体的用户，这种能力使得产品具备从用户业务的视角对安全事件进行调查、回溯。

4.2 用户认证令牌防护

产品通过对用户认证相关信息进行加密与重放保护，防止攻击者对用户认证相关信息进行篡改、窃取与重放，保证用户认证信息的安全存储与使用。

4.3 用户业务逻辑漏洞安全防护

当网站存在业务漏洞时，攻击者可能利用该漏洞提升自身权限或访问未授权的网站资源。产品密切监控业务用户的权限状态，实时检测用户权限状态的异常变化，及时阻断异常授权的访问。

4.4 基于用户业务的访问控制

基于产品的用户身份识别和跟踪能力，实现从用户业务层面进行访问控制，支持禁止某一用户对特定业务的访问控制。

为业务系统注入“疫苗”

在攻防演练场景中，为了保障应用程序安全，通常会部署多种安全防护产品，其中最为常见的是的基于流量检测类的安全设备，例如 WAF 产品。该类产品就像是给业务系统戴上了“口罩”，可在应用外侧提供防御，并对流量进行过滤清洗，但应用本身对“威胁”是缺少感知的。

这种防御方式，虽然对于攻击方的扫描行为或者是攻击尝试，都能进行识别和发现，但在庞大的流量告警场景下，对于中间是否穿插有攻击成功的请求，就需要有安全专家根据响应包以及经验来进行二次的研判分析，甚至进一步定位到业务系统现场，在主机层面进行排查。更极端的情况是，若遇到高水平攻击者使用针对性的混淆、变形手段，甚至是 0day 漏洞攻击来绕过流量安全设备，此时的攻击行为就更难被发现了，就只能依靠主机层面的防护措施或一些后续通用流量特征来识别了。

归根结底，“口罩”模式的防御方法，毕竟不是应用本身的一部分；而能及时感知和确认自身遭遇“威胁攻击”的最佳“位置”，还是应用本身。

安天应用威胁自免疫（以下简称：Antiy RASP）作为应用运行时的自我防御工具，可以在应用内部对攻击进行识别与防御，即为业务系统增加自我防护与免疫能力的一剂“疫苗”。



图 1 WAF + Antiy RASP 对应用系统的双重防护模式示意

在攻防演练前，为应用系统注入 Antiy RASP，可在传统“口罩”模式防御基础上补充自我免疫“威胁”的能力，形成双重防护模式，切实有效地阻止“远程命令执行”、“上传 WebShell”等重症的发作。

1. Antiy RASP 设计原理

Antiy RASP 与应用紧密结合，在关键函数执行前进行安全检测，为应用自身赋能安全防护能力，低误报，高检出地智能拦截各类已知及未知漏洞，并提供漏洞成因管理、报警通知、安全检查等多种能力。具有高性能、高兼容性，部署便捷的特性。

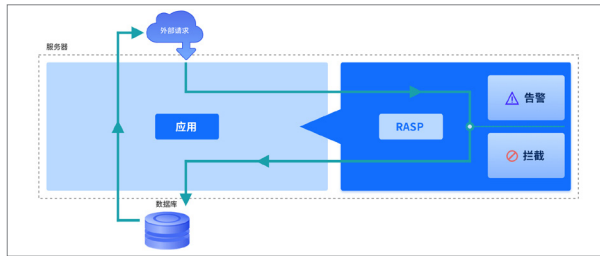


图 2 Antiy RASP 设计原理示意图

可在无定制化的情况下，支持 HTTPS 业务、自加密请求场景的防御。针对高水平、变形绕过的攻击，甚至 0day 漏洞攻击，Antiy RASP 可基于行为特征进行有效检测，并精准定位漏洞详情。

2. 五大攻防演练场景价值（Q&A）

问题 1：攻防演练期间，陈旧、缺乏维护的业务系统是被攻击的重点目标，但又要保证其正常运行，怎么办？

Antiy RASP：为陈旧的应用系统嵌入最新的安全检测代码，在不影响业务的正常运行的前提下，提供安全防护。

问题 2：攻防演练期间出现了 0day 漏洞，高水平的攻击者可能绕过防御设备，在相关对策还不完善的情况下，该如何有效防御？

Antiy RASP：基于行为特征的通用漏洞检测算法，可作为应对 0day 漏洞的兜底手段，极大提高应用安全防护能力的短板。

问题 3：应用系统的数据使用了加密数据传输，未做定制化的流量安全设备无法解密则无法防御？

Antiy RASP：因注入位置的特性，使其可以对解密后、格式化后的数据进行研判分析，精准识别攻击者的意图，而不受混淆绕过、加密请求的干扰。

问题 4：如何在应急处置过程中得分，以最快的速度获得漏洞定位与修复能力，以及业务整改恢复能力？

Antiy RASP：在成功实现攻击防御后，可以知晓恶意行为是如何产生，漏洞是如何造成的。不仅可以帮助后续修复，也可支撑及时为同类应用修复与响应。

问题 5：1day 漏洞详情公布了，如何快速自查应用依赖是否在受影响清单中？

Antiy RASP：通过组件管理功能，可确认应用依赖的版本信息。

3. 有效适配演练场景

Antiy RASP 采用探针 + 平台管理的方式，平台支持 SaaS 化部署和私有化部署两种方式。

3.1 管理平台：提供探针的统一管理

SaaS 化部署：只需在安天垂直响应服务平台上申请开通后，创建对应的企业租户即可使用。

私有化部署：支持容器化、非容器化多种部署方式；适用于探针无法出网的情况。

3.2 探针（Agent）：嵌入到应用内部，为应用提供安全防护能力

JAVA 语言支持 Windows / Linux，JDK7-17，OracleJDK / OpenJDK，Tomcat / Spring Boot / Jboss / PHP /...等环境的任意组合。

PHP 语言支持 Linux 环境下 5.4、5.5、5.6、7.0、7.1、7.2、7.3、7.4 版本。

同时，提供一键安装脚本（程序）和安装镜像，可在不重启应用的情况下，动态注入到需要被保护的主机进程、Docker 容器、Kubernetes 集群。并支持引擎热更新。

4. 重点能力支撑演练需求

4.1 智能拦截各类已知及未知漏洞

使用 Hook 技术对各类关键函数进行监测，根据用户输入、已知规则等对函数调用进行污点追踪和快速检查，自动拦截风险调用并提示运维和开发人员。支持拦截 48 种类型攻击（JAVA 语言 23 类、PHP 语言 25 类），覆盖绝大多数常见漏洞。

4.2 可追溯到具体漏洞点

每次攻击事件均会详尽地记录相关信息，包括全部的用户输入、完整的请求信息、触发的漏洞类型、格式化后的攻击 Payload、触发漏洞时应用的瞬时堆栈信息、

涉及的资产信息，并提供修复建议。帮助开发人员快速准确定位并修复漏洞。

4.3 组件管理

应用依赖库信息统一展示，方便定位是否存在供应链污染问题。

4.4 应用加固与安全检查

通过浏览器的安全特性，通过输出指定响应头实现对应用的加固。

检查应用程序安全运行所需的相关配置，包括弱口令检测、默认配置检测、安全运维项检测等。

快速开展应急处置与分析取证

在攻防演练期间，针对突发的恶意威胁攻击事件，需要快速开展应急处置与分析取证工作。此时，具备应急处置、分析取证能力的工具箱将显著提高工作效率，甚至发挥出难以替代的重要作用。

安天拓痕应急处置工具箱（以下简称：拓痕工具箱）正是一款适用于上述场景的便携式工具箱，其核心部件包含：主机深度分析处置工具、应急处置主机等。拓痕工具箱内置国产化自主可控的威胁检测引擎，集成了安天在系统安全监测与处置、流量安全分析、恶意代码行为分析及应急响应等领域的多年技术积淀与实战能力，能够有效支撑攻防演练期间的防守保障。

1. 攻防演练价值

便携式工具，界面简洁易用，无需安装，即插即用。
具备对威胁事件的快速响应处置能力，增强应急响应和分析处置能力。

2. 演练场景适配

2.1 安全巡检

拓痕工具箱内的主机安全检测系统，依托安天强大的基础引擎和自研安全驱动，可以全面分析系统面临的安全隐患与威胁。模块输出的分析报告内容详实，便于安全管理人员掌握全网资产的安全状态，满足多场景安全巡检的工作需要。

2.2 恶意代码检测

依托安天 20 余年专业反病毒经验与能力积累，通过快速取证，可以对目标机的自启动项、进程、线程、句柄、端口、内核信息、MBR、插件、钩子、系统文件等关键位置进行全方位的检测，通过云端检测、本地引擎形成对各检测对象的威胁等级判定。

2.3 应急响应与处置

拓痕工具箱全部功能实现均基于 ring0 级进行开发研制，对目标主机拥有最高级别的分析处置权限，通过恶意代码检测模块检出的关键信息，使用底层驱动技术对自启动项、磁盘引导扇区、系统用户、端口、服务、进程、内核模块、消息钩子、内核钩子、SSDT、注册表等系统关键位置进行恶意攻击行为分析，并提供相应的应急处理手段。面对复杂的恶意入侵，拓痕工具箱可以

提供强力的应急处置手段，保障受攻击的业务系统得到快速处置和恢复、加固，降低其再次受到攻击的风险。

3. 产品能力支撑

拓痕工具箱可广泛应用于网络安全事件的应急响应、威胁检测、分析、处置、取证及 IT 系统紧急运维等场景。拓痕工具箱完全由安天自主研发，融合安天核心引擎与 20 余年威胁对抗经验，产品安全可控，操作简单易用，在终端侧打造集安全检测、深度分析、证据提取、问题处置于一身的实用工具，形成闭环操作，有效应对安全事件各环节需求，面对威胁既可未雨绸缪、防患于未然，又能够应对有方、防微杜渐。

主机安全检测模块由便携式专用 USB 设备或光盘承载，界面简洁易用，无需安装，即插即用。基于国产化自主可控的威胁检测引擎（AVL-SDK）和威胁情报的扩展，

实现了海量恶意代码检测和精准命名能力，并形成一定的未知威胁发现能力。能够在主机侧实现安全检测、深度分析、证据提取、问题处置的闭环操作，辅助安全人员对安全事件的全生命周期开展调查取证工作。

应急处置功能针对顽固感染中的多进程/线程保护、驱动级保护，以及 Rootkit 木马的隐藏点，设计了灵活的挂载内核驱动提取与处置机制，对目标终端具有高级别的分析处置权限，且在网络安全事件中具备底层的处置能力。

同时，通过联动“探海威胁检测系统”可对终端防护软件未检出恶意威胁进行定位取证，对恶意威胁形成初步分析，对安天多产品进行知识输出；通过联动“安天追影威胁分析系统”对未检出的恶意威胁进行详细分析，可有效支撑分析人员分析恶意威胁攻击方式及逻辑，从而进行有效、快速的业务系统加固。

附录：

安天产品攻防演练价值表		
防护类别	安全产品	产品价值
终端防护	智甲终端防御系统	安天智甲终端防御系统内置安天自主研发的下一代威胁检测引擎，基于黑白双控模式的安全策略，有效支撑终端检测与响应。智甲融合了主机防火墙、终端管控、外设管控、漏洞扫描、集中补丁修复等管理功能，结合安天独家的高级威胁追溯包服务，可以实现全网威胁追溯。在攻防演练中，智甲可有效检测和抵御落地到终端侧的攻击。
云主机防护	智甲云主机安全系统	安天自主研发的面向多云、混合云的云主机安全系列产品，帮助客户建设以资产安全为核心、风险防范为重点、安全事件为驱动的统一云安全运营管理体系，能够为客户提供一站式云安全防护，全面提升云安全建设水平。在攻防演练中，云主机安全系统可精准检测外部威胁、内部风险，防护云中资产安全。
全流量威胁检测	探海威胁检测系统	安天探海威胁检测系统能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁，并可与安天威胁情报服务结合，对多个 APT 攻击组织的载荷工具和 C2 基础设施实现带有精确组织指向的报告告警。在攻防演练中，探海可多层次多维度检测，提升威胁发现能力，有效提高威胁分析响应速度。
威胁分析	追影威胁分析系统	安天追影威胁分析系统借助包括安天下一代检测引擎在内的多组鉴定机制组合对输入对象进行判定分析，可有效检出分析鉴定各类已知与未知威胁，尤其对基于格式文档的 0day 漏洞攻击具备优秀的检出能力，深度揭示威胁行为细节，输出详实报告。在攻防演练中，追影可有效检出高级威胁，并与安全产品联动，增强整体安全防护能力。

安天产品攻防演练价值表		
防护类别	安全产品	产品价值
威胁捕获	捕风蜜罐系统	安天捕风蜜罐系统是部署在网络环境中用于诱骗攻击者的设备级主动防御型网络安全系统，可模仿多种系统环境，及时感知攻击从而进行预防，能够捕获攻击者利用的攻击工具并记录攻击全过程。在攻防演练中，捕风可诱捕攻击方的攻击行为，为反制攻击方提供有效支撑。
威胁情报	威胁情报分析平台	安天威胁情报分析平台可以有效支撑安全事件分析工作，针对攻击者的攻击工具、攻击资源、攻击手段进行全面揭示，形成了追踪溯源的能力，最大程度的减少搜集情报和威胁分析时间，在关键系统和数据受损之前最大程度地缩短事件响应时间并中断杀伤链。在攻防演练中，威胁情报分析平台可为客户提供精准的威胁情报，协助安全分析人员对攻击事件追踪溯源。
应急处置	拓痕应急处置工具箱	安天拓痕工具箱作为便携式工具，内置安天下一代威胁检测引擎，集成了安天多年系统安全监测与处置、流量安全分析、恶意指码行为分析及应急响应积累的技术和能力，能够实现安全运维的日常检查和快速的应急处置。在攻防演练中，拓痕可协助安全分析人员快速取证，高效定位事件目标，为应急处置提供支撑。
边界阻断与入侵防护	镇关下一代防火墙	安天镇关防火墙从用户、应用和行为的角度出发，在传统防火墙功能基础上，提供用户策略、应用策略和行为策略等智能控制手段，有效解决了传统防火墙无法解决的问题。在攻防演练中，镇关可以有效的补充边界防护，在边界形成综合的深度防御，阻断攻击行为。
脆弱性发现	安天漏洞扫描系统	安天漏洞扫描系统具备完善和高效的脆弱性扫描能力，可通过集中管理、周期性扫描等，从多个维度对网络环境中所有系统或网站进行脆弱性扫描和整体评估分析，并提供加固方案。在攻防演练中，漏扫系统可有效开展大范围安全检查，帮助客户快速检测资产漏洞。
网站安全防护	WEB 应用防护系统（WAF）	安天 WEB 应用防护系统（WAF）针对安全事件发生时序进行安全建模，分别针对安全漏洞、攻击手段及最终攻击结果进行扫描、防护及诊断，提供综合 WEB 应用安全解决方案。在攻防演练中，WEB 应用防护系统可针对 Web 业务应用进行有效防护，发现和阻断针对性的 Web 攻击。
	应用威胁自免疫 Antiy RASP	Antiy RASP 与应用紧密结合，在关键函数执行前进行安全检测，为应用自身赋能安全防护能力；低误报，高检出地智能拦截各类已知及未知漏洞，并提供漏洞成因管理、报警通知、安全检查等多种能力。具有高性能、高兼容性，部署便捷的特性。在攻防演练中，可以在 WAF 基础上补充自我免疫“威胁”的能力，形成双重防护模式，切实有效地阻止“远程命令执行”、“上传 WebShell”等重症的发作。
态势感知	鉴形态势感知平台	安天鉴形态势感知平台包含了资产安全运维、安全设备管理、甄别研判、指挥联动、知识与情报等组件，在兼顾结合面与覆盖面、不断完善强化已有静态防御机制的同时，打造动态综合的网空安全防御能力体系。鉴形能高效地实现威胁与脆弱性检测识别、安全事件理解分析、攻击与影响预测、协同联动处置、情报与知识生产，实现安全态势的全面感知与安全业务的融合贯通，对复杂的网络攻击进行更为精准地发现与打击。在攻防演练中，鉴形态势感知平台可面向敌情、我情、战情呈现态势，加速自动甄别与人工研判，全面支撑演练期间的安全防御体系。

04 安天党建文化与青春风采

近年来，安天将思想政治和组织文化工作有效整合，坚持以一体化的理念谋划党建工作，以一体化的思路优化资源配置，以一体化的方式推动文化建设，以文化引领、保障打赢、服务一线、聚焦基层和鼓励奋斗为基本工作目标，为集团实现高质量发展提供支撑。

本章内容分享了安天在纪念“4.19”网络安全和信息化工作座谈会六周年、“7.1”建党节组织的相关活动，展现了安天人在网络安全工作一线的精神风貌和青春风采。

在此，感谢安天集团党委、各属地党支部、组织文化部、品牌管理部等相关人员对本章内容所做出的贡献。

庆祝中国共产党成立 101 周年，喜迎党的二十大胜利召开——安天集团组织开展系列庆祝活动

多年来，安天坚持以党建促发展，始终把党建作为集团发展的“红色引擎”，以高质量党建助推集团高质量发展，实现党建与经营互促共进。2022 年，安天将思想政治和组织文化工作有效整合，坚持以一体化的理念谋划党建工作，以一体化的思路优化资源配置，以一体化的方式推动文化建设，以文化引领、保障打赢、服务一线、聚焦基层和鼓励奋斗为基本工作目标，为集团实现高质量发展提供支撑。

2022 年 7 月 1 日，在中国共产党的 101 周年华诞到来之际，安天集团党委以丰富的形式开展庆祝中国共产党成立 101 周年系列活动，以实际行动迎接党的二十大胜利召开。

1. 组织召开全体党员大会

在集团党委的统一组织下，各党支部开展奏国际歌、党员宣誓等活动，重温入党誓词；对本年度在研发攻关、应急响应等方面工作突出的优秀共产党员及党务工作者予以表彰；以“不忘初心、牢记使命”为主题，结合“百年科技强国梦”等视频资料，开展专题党课活动，进一步激励广大共产党员坚定信念、对党忠诚，履职尽责、奋发有为，将此汇聚成推动公司快速健康发展的强大正能量。

2. 组织“巾帼心向党 共同庆华诞”主题活动

在集团党委的统一组织下，各属地工会委员会组织



图 2 安天开展“巾帼心向党 共同庆华诞”主题活动

女员工，开展了“巾帼心向党 共同庆华诞”主题活动，通过读书分享和手工制作的方式，表达对党的赤诚之心和感激之情。一幅幅精美的手工作品不仅融入了安天人对党的无限热爱，更表达了对党的美好祝愿，用最质朴的行动表达“永远跟党走”的信心和决心，在党的光辉映照下，奋勇向前，用网络安全人的实际行动践行初心和使命。

3. 安天精品党课登上央视《焦点访谈》

在当晚播放的央视《焦点访谈》中，以《党旗在一线飘扬 百年大党正青春》为主题，展示了中国共产党作为百年大党始终生机勃勃，带领中国人民创造一个又一个奇迹。一个历经百年风雨与磨难的大党，因重视学习、



图 3 工作人员在安天拍摄精品党课
善于学习而始终保持着蓬勃向上的青春活力。

其中，在安天集团拍摄的以《牢记习近平总书记嘱托 为数字经济发展保驾护航》为主题的安天精品党课内容和拍摄现场环节登上《焦点访谈》，成为不断增强党课的吸引力和感染力的案例。



图 1 各党支部组织召开全体党员大会

纪念“4·19”重要讲话六周年 安天开展“总体国家安全观”宣传月活动

六年前的4月19日，习近平总书记召开了网络安全和信息化工作座谈会，发表了重要讲话，为网络强国战略目标构建了方法论工作指引。安天创始人肖新光同志作为十名发言代表之一，代表网络安全产业向总书记汇报。六年来，安天人承载使命，攻坚克难，实时跟踪威胁对抗态势，聚焦技术创新与核心能力生成，取得了一定工作成绩。

安天党委在每年4月~5月，组织系列与工作实践相结合的思想政治学习活动，也成为例行传统。安天在践行初心使命、加强自主创新的同时，深入贯彻执行“总

体国家安全观”，有序组织开展了“总体国家安全观”宣传月活动的各项工作。

1. 党课学习强化思想引领

安天各地党支部组织观看了“4.19”讲话央媒报道视频，组织大家重读习近平总书记“4.19”讲话，学习《习近平关于网络强国论述摘编》、《习近平关于总体国家安全观论述摘编》等重要资料，强化思想引领，达到思想上、政治上、行动上的高度一致。通过此次学习活动，每位党员都认真领会了“总体国家安全观”的重大意义、



图1 各地党支部组织观看“4.19”讲话央媒报道视频

丰富内涵与实践要求，同时更加明确安天相关技术能力的实施方向和目标。

2. 专题学习深化国家安全意识

安天集团党委上线了“总体国家安全观”内部学习专题，引导广大员工对习近平总书记4.19重要讲话内容的深入学习，一同回顾习近平总书记就维护国家网络安全发表的一系列重要论述，对广大员工深化国家安全意识、提升国家安全理念具有重要的意义，进一步增强了安天人维护国家网络空间安全的责任感和使命感。



图2 安天官网上线“总体国家安全观”学习专题

3. 张贴宣传资料丰富学习方式

安天各地党支部在宣传专区张贴国家安全教育宣传海报、宣传标语，通过多种方式宣传“总体国家安全观”的核心要义、危害国家安全的主要行为表现及典型案例、维护国家安全的注意事项及应对措施等方面内容，为员工深入学习“总体国家安全观”提供了多种途径，切实做到将“总体国家安全观”深入人心。

4. 知识竞赛检验学习成效

在安天集团党委的指导下，安天集团团委、组织文化部联合组织开展了“‘安天奋斗好青年 国家安全先锋队’总体国家安全观知识竞赛”活动。本次竞赛围绕“总体国家安全观”的提出背景、基本内涵、重要意义等内容开展，旨在指引全体员工自觉强化对“总体国家安全观”的理解，自觉遵守国家安全法，自觉防范各类安全风险，自觉提升安全防御技能。安天各属地公司员工积极参与，

经过激烈角逐，最终评选出一等奖20名、二等奖30名、三等奖50名，优秀组织部门3个。

5. 网络安全极限技术挑战赛圆满落幕

为进一步提升工程技术人员面向威胁挑战的敌情意识和实战化能力，安天举办了一场网络安全极限技术挑战赛，经过连续48小时的巅峰对决，比赛已经圆满落幕。与往届相比，本届比赛将编程开发与威胁分析分为两组同步进行，客观上降低了参赛的技术栈门槛，避免让编程高手或分析高手因担心遇到自己的技术短板而放弃参赛。同时，比赛的难度要求大幅提高，对编程作品提出了更为严格的功能、性能指标要求，对于分析题目则最大限度地仿真了实战场景。比赛自今年5月下旬起报名，共吸引近百名工程师参与，参赛战队及参赛人数都创下历史新高。



图3 网络安全极限技术挑战赛比赛现场

通过开展网络安全极限技术挑战赛，进一步激发了工程师的学习热情，增加了网络安全行业人才储备，巩固了安天在高级威胁分析和网络安全专业技术领域所取得的成果。参加比赛的安天工程师表示，本次活动不仅提高了员工在网络安全威胁分析方面的专业技能，也让我们充分认识到网空威胁的挑战和压力，更加深刻地感受到作为网络安全工作者所肩负的责任和使命。

逐梦新青年，我们正青春

习近平总书记指出：“中国共产党自成立之日起，就始终把青年工作作为党的一项极为重要的工作。”100年来，我们党始终从确保党的事业薪火相传、确保中华民族永续发展的战略高度看待青年工作，以崇高初心使命感召青年，以科学思想理论武装青年，以不懈奋斗精神激励青年，以广阔事业舞台成就青年。

2022年，是中国共产主义青年团成立100周年，回望百年，青春向党。让我们一同倾听安天新一代青年在网络安全工作一线挥洒青春的故事，感受他们在运动场上奋力拼搏、激扬青春。

1. 安天新一代青年眼中的青春

在安天有这样一支英勇善战的队伍，他们凭借自身在网络安全领域的专业能力来保卫国家安全和国家发展，他们长期与境内外网络攻击威胁进行对抗，他们就是安天网络民兵分队。作为全国唯一一支百人规模的网络民兵队伍，他们肩负的一项重要职责是防范境外敌对组织对我国发起网络攻击。

高喜宝是安天网络民兵分队中的一员，他及时发现了利用疫情信息传播的恶意代码，并提出解决方案。他说：“每拦截一个恶意代码，每进行一次威胁分析，都是一份坚守，一种荣耀，民兵成员要不断丰富自身的知识和技能，同时具备忠于国家，敢于奉献，不惧牺牲的勇武精神。”他热爱骑行，曾带队骑行全国多个省份，这些经历让他更坚毅，更加无所畏惧。

他眼中的青春

走过崎岖泥泞的山路，骑过水天一色的海岸；翻过南北横亘的山脉，望过一马平川的草原；在不断前行的路上，是一个个的目标、不断优化的方法、用尽毅力的坚持，成就不悔的青春。

同样在与高级威胁持续对抗的还有安天应急响应中心邢宝玉，作为一名党员，邢宝玉用实际行动践行初心使命，多年来专注于网空高级威胁研究分析工作，对APT组织活动进行分析溯源并积极参与WannaCry、CPU 0day等多个事件的应急响应工作，全力确保各项任务圆满完成。除此之外，他不断提高钻研和创新能力，牵头推动专利申请工作，提交多项APT相关发明专利。在这个没有硝烟的战场上，他执着专注，奋进致远。

他眼中的青春

青春，是永不停歇的热忱，是勇于开拓创新，是对一个目标的执着追求。

国家重大活动期间，作为7*24小时守护客户安全中的一员，张康曾为重保项目连续出差5个月，针对互联网出入流量进行综合分析，全方位监测流量态势，协助客户打造了一个安全平稳的网络环境。他通过专业服务、真诚付出，最终获得了客户的信赖和赞誉。他对“做什么样的青年人”有自己深刻的思考和定位，他希望青春像一颗耀眼之星，有棱角，会发光。

他眼中的青春

拥有过硬的技术，具备吃苦耐劳的精神，希望青春会发光。

来自终端安全团队的崔阳，全力坚守威胁防御的最后一道防线，他多次参与国家重大任务的安全保障工作，扎实做好每一个项目的系统对接与兼容性测试，第一时间协调处理安全隐患。在病毒威胁事件处置中，他连夜赶赴客户现场进行勘查，耐心沟通用户需求并协调公司资源，提供先期解决方案，有效解决了客户的安全风险。

他坚信习总书记对网络安全工作的重要指示“没有网络安全，就没有国家安全”，网络安全是信息时代国家的“网络空间领土”，我们作为网络安全工作者更应从国家安全的战略高度认识网络安全。

他眼中的青春

青春是朝气蓬勃，是激情澎湃，是斗志昂扬。

青春要锤炼品格、脚踏实地、敢为人先。

现在，青春是用来奋斗的，将来，青春是用来回忆的！

了产品研发过程中的实际困难。无数个深夜，他和研发人员一起挑灯攻克难关，努力保障流量产品国产化的创新性和可靠性。在自身取得进步的同时，他的强执行力也不断带动和影响了团队成员。

他眼中的青春

青春是充满无限激情和力量的，只有真正挥洒过汗水，

绞尽过脑汁，竭力奋斗，才能不负韶华。

一方有难，八方支援。新冠疫情爆发后，安天启动重大社会事件网络安全应急值守制度，众多青年工程师放弃休息时间，全力参与到保障医疗系统安全的工作中，提供免费安全咨询和应急响应服务。在武汉洪灾、



图1 安天员工青春风采

河南水灾等多次自然灾害事件发生后，安天集团党委第一时间统筹谋划支援行动，全体安天人踊跃捐款，其中，青年人成为带动捐款的主力军，在危难时挺身而出，贡献了青春力量。

在共同抗“疫”的特殊时期，安天各地青年党员代表积极发挥引领作用，在宣传疫情防控措施的同时，积极号召大家配合测温、消毒，并有序组织核酸检测工作。

他眼中的青春

青春是一份带有温度的关爱，是面临严峻考验时的坚强，是团结互助，攻坚克难，是风雨同行，共渡难关。

他们用微光照亮四周，用最美的青春诠释担当。

青春是多彩多面的，每个人的青春以及他们对青春的理解都是不同的，但他们的共同点是兢兢业业、忠于职守、敢于拼搏、勇于创新、甘于奉献，他们在各自的工作岗位上热忱地奉献自己的青春与智慧。作为安天人，我们很荣幸与无数勇士一同守护国家网络安全，我们奋斗在路上，我们正青春。

2. “羽”你同行，只因热爱——安天成功举办“安小虎”杯羽毛球友谊赛

为进一步丰富员工业余文化生活，增强团队凝聚力，

7月15日，北京安天举办了2022年度“安小虎”杯羽毛球友谊赛。组织部门为此次活动做了充分的准备，从策划到正式比赛共历时一个月，以会议讨论的方式确定了比赛流程、比赛规则以及相关工作人员的职责，同时，为参赛选手准备了精美的奖品。

七月的北京，暑气蒸腾，宝海羽毛球馆蓝色的屋顶下，洋溢着热烈的青春气息，这是北京安天羽毛球俱乐部成立后的第一场赛事，来自北京安天的24位小伙伴齐聚宝海羽球会，分成ABCD四个小组进行团体的循环对决，平日里以严谨著称的工程师们在赛场上激烈角逐、尽展活力。这不仅是体力、耐力、技巧、趣味的比赛，也是

策略、战术、合作的竞争。选手们斗志昂扬，在团队的相互配合中细心总结经验、扬长避短，一记记精彩的扣杀、巧妙的吊球赢得场下连连叫好，激烈的比赛氛围感染着每一个人，最终C组凭借出色的发挥获得冠军。

场上挥汗如雨，场下欢笑不断，通过举办本次比赛，进一步增强了安天员工对羽毛球运动的认识，点燃了大家对体育运动的热情，充分展现了安天人的青春活力、积极向上的生活态度和努力拼搏、不断进取的精神风貌，同时，增进了员工之间的友谊和团队凝聚力。



安小虎简介

安小虎作为安天个人安全产品代言人，为个人/家庭和中小企业用户提供专业安全服务，包括：个人安全产品和响应服务、个人安全知识条漫、个人安全专题资讯和个人安全咨询服务等，目前已为个人/家庭和中小企业用户提供安天垂直响应平台、安天杀毒、密码钱包、数据保险箱、勒索风险检测和专项服务、文件深度分析服务等产品与服务，致力于保护个人/家庭用户和中小企业资产和数据安全。



扫描二维码
了解安天更多个人安全产品



图2 “安小虎”杯羽毛球友谊赛现场

安天资讯 INFORMATION

No1 | 安天接受《焦点访谈》采访 | 筑牢网络安全基石 维护国家安全

4月15日，第七个全民国家安全教育日，央视《焦点访谈》特别播出“国家安全，共同守护”专题节目，安天创始人肖新光 and 副总工程师关墨辰接受采访，介绍网络安全风险形势与挑战。



No2 | 安天移动安全在 2022 年 AV-TEST 测评中再次领跑国际第一梯队

近期，德国权威安全机构 AV-TEST 公布了 2022 年 5 月份移动安全软件测试测评最终的测试成绩，安天移动安全再次以实时测试、常规测试检出率双 100% 检出率，以及检测能力、可用性、性能表现各 6 分，总分满分 18 分的完美成绩，在移动安全领域继续领跑国际第一梯队。

Android: May 2022				
Product	AVG 5.0	Confidential	Protection	Performance/Usability
Antiy	100%	6	6	6
Avira	100%	6	6	6
Kaspersky	100%	6	6	6
AhnLab	100%	6	6	6
McAfee	100%	6	6	6
Avast	100%	6	6	6
Bitdefender	100%	6	6	6
Google	100%	6	6	6
Play Protect	100%	6	6	6
Avast	100%	6	6	6
Avast	100%	6	6	6

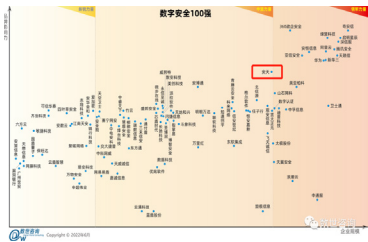
No3 | 安天收到公安部网络安全专项行动感谢信

近期，公安部向安天发来感谢信，充分肯定了安天在 2021 年公安部网络安全专项行动中所做出的积极贡献。在本次任务中，安天积极配合，组织专业力量，调动资源，充分发挥自身优势，以专业的技术水平和职业素养全面支持专项行动，并圆满完成任务。



No4 | 安天入围网安百强“中坚力量”企业首位

6月18日，第三方调研与咨询机构数世咨询发布《2022 年中国数字安全百强报告》。安天在“综合实力百强”中，以较高的影响力和高速发展力占据“中坚力量”显著位置，成为拟上市企业阵营的重要力量，并获得年度增长力十强企业。



No5 | 安天参写《2021 网信自主创新调研报告》发布

4月19日，由《网信自主创新调研报告》编委会主办的“第五届关键信息基础设施自主安全创新论坛暨纪念习近平总书记‘4.19’讲话发表六周年活动”在京召开。会上，正式发布《2021 网信自主创新调研报告》，并公布了 2022 “网信自主创新先锋企业”。安天参与编写“反恶意代码引擎”及“高级威胁检测”章节，同时被评为基础软件、安全服务、计算环境安全、云计算安全等多个领域的“网信自主创新先锋企业”。



No6 | 安天参编《数据安全法》实施参考（第一版）发布

中国网络安全产业联盟数据安全工作委员会在中国网络安全产业联盟、全国信息安全标准化技术委员会秘书处指导下，组织编制《〈数据安全法〉实施参考（第一版）》已于 2022 年 4 月正式发布。安天作为主要参编单位，为《实施参考》的顺利编制、发布提供了重要支持。



No7 | 安天排名第 20 位 | 入选“2022 年中国网安产业竞争力 50 强”

6月23日，由中国网络安全产业联盟（CCIA）发布、数说安全提供研究支持的“2022 年中国网安产业竞争力 50 强”正式揭晓，安天连续两年以排名第 20 位入选“2022 年中国网安产业竞争力 50 强”。



No8 | 《嘶吼 2022 网络安全产业图谱》发布 安天入选全部六大类别

7月13日，嘶吼安全产业研究院联合国家网络安全产业园区（通州园）正式发布《嘶吼 2022 网络安全产业图谱》。安天以覆盖全部六大类别，38 个二级分类，61 个细分领域，入选二级细分领域 TOP11 网络安全厂商；并以第二位排名入选 2021 年发布新品（含产品版本）最多的网络安全厂商。





2022年6月6日，
是安天22周年的生日。
回首过去的峥嵘岁月，
我们风雨兼程，
一路同行；
展望未来的美好蓝图，
我们坚定信念，
斗志昂扬。
期待安天的明天，
更加闪亮！

品牌部 张丽（绘）

国产自主
威胁检测引擎

易管理、降成本

多维度防勒索、防挖矿

APT高级威胁防护

全感知、快响应

全终端
场景适配

私有云查杀
黑白双控

强能力、建体系

智甲

安天智甲终端防御系统

安全之本 有效防护

安天智甲终端防御系统（英文简称：IEP）基于UES（统一端点安全）理念研发，将病毒查杀、配置加固、可信环境验证、主动防御、分布式防火墙、外设管控、Web Server防护等模块积木化组合，可以有效覆盖包括传统桌面、工作站、服务器、虚拟化、容器等场景的安全需求，对包括Windows、Linux、Android以及欧拉、麒麟、统信等国产操作系统都能有效建构系统内核层防御。广泛用于政府、公安、金融、交通、能源、电信、医疗、制造、教育科研、军队军工等各行业。



安天官方微信



安天开放资料平台

北京运营总部

地址:北京市海淀区闵庄路3号
清华科技园玉泉慧谷一期1号楼
邮编:100195

成都、武汉、深圳、上海、沈阳、南京六地研发中心

内部资料 赠阅参考

哈尔滨总部基地

地址:哈尔滨市松北区世坤路838号
科技创新城7号楼
邮编:150028