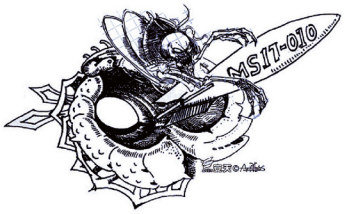
安天周观察

主办：安天　2017 年 5 月 15 日（总第 87 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

勒索者蠕虫病毒 WannaCry 专题

安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发

安天已经正式为 WannaCry 命名为“魔窟”，“魔”可以表示该威胁的严重性，“窟”表示利用永恒之蓝相关严重漏洞传播的特点。



安天安全研究与应急处理中心 (Antiy CERT) 发现，北京时间 2017 年 5 月 12 日 20 时左右，全球爆发大规模勒索软件感染事件，我国大量行业企业内网大规模感染，教育网受损严重，攻击造成了教学系统瘫痪，甚至包括校园一卡通系统。截止到 5 月 13 日 23 时，病毒影响范围进一步扩大，包括企业、医疗、电力、能源、银行、交通等多个行业均遭受不同程序的影响。

经过安天 CERT 紧急分析，判定该勒索软件是一个名称为“WannaCry”的新家族，目前无法解密该勒索软件加密的文件。该勒索软件迅速感染全球大量主机的原因是利用了基于 445 端口传播扩散的 SMB 漏洞 MS17-010，微软在今年 3 月份发布了该漏洞的补丁。2017 年 4 月 14 日黑客组织 Shadow Brokers（影子经纪人）公布的 Equation Group（方程式组织）使用的“网络军火”中包含了该漏洞的利用程序，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了此次全球性的大规模攻击事件。

安天 CERT 在 2017 年 4 月 14 日发布的《2016 年网络安全威胁的回顾与展望》中提到“网络军火”的扩散全面降低攻击者的攻击成本和勒索模式带动的蠕虫的回潮不可避免等观点。结果未满 1 个月，安天的这种“勒索软件 + 蠕虫”的传播方式预测即被不幸言中，并迅速进入全球性的感染模式。

安天依托对“勒索软件”的分析和预判，不仅能够有效检测防御目前“勒索软件”的样本和破坏机理，还对后续“勒索软件”可能使用的技巧进行了布防。安天智甲终端防御系统完全可以阻止此次勒索软件新家族“WannaCry”加密用户磁盘文件；安天探海威胁检测系统，可以在网络侧有效检测针对 MS17-010 漏洞的利用行为；安天态势感知系统，基于有效感知全局资产脆弱性和受损态势的基础上，能快速联动做出全网追溯、补丁加固、系统免疫等响应处置，有效缩短响应时间。

【响应轨迹】

5 月 12 日

20:20，决定启动“A 级灾难”响应。

22:45，经测试，安天智甲终端防御系统无需升级即可有效阻断 WannaCry 加密行为、安天探海威胁检测系统升级后可以检出 WannaCry 的扫描包。

5 月 13 日

06:00，发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》深度分析报告，微信公众号一天突破 31 万的阅读量。

5 月 14 日

04:49，发布《安天应对勒索者蠕虫病毒 WannaCry FAQ-2: 传言验证者》。

05:00，发布《安天应对勒索软件 WannaCry 开机指南》，该病毒爆发于北京时间周五晚 8 点，周一开机将成为一场安全考验。

05:22，更新《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》深度分析报告。

17:00，国家网信办网络安全检查共享平台，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

18:00，公安部共享平台，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

18:44，安天和友商应急团队联合讨论，将 WannaCry 中文俗名确定为“魔窟”。

19:00，发布安天智甲防勒索免费版。

20:00，更新发布免疫工具、专杀工具。

17:25，发布《安天应对勒索软件 WannaCry 配置指南》。

17:45，发布《安天应对勒索者蠕虫病毒 WannaCry FAQ-1》，针对大量用户的高频问题进行回复。

19:03，发布 WannaCry 免疫工具和扫描工具。

19:03，公安部下属国家计算机病毒应急处理中心，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

20:00，国家互联网应急中心发布《关于防范 Windows 操作系统勒索软件 Wannacry 的情况通报》，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

5 月 15 日

凌晨，更新发布《安天应对勒索软件“WannaCry”开机指南》。

勒索者蠕虫病毒 WannaCry 专题

【思考建议】

勒索软件给国内政企网络安全带来了新的挑战。在较长时间内，国内部分政企机构把安全的重心放在类似网站是否被篡改或 DDoS 等比较容易被感知和发现的安全事件上，但对网络内部的窃密威胁和资产侵害则往往不够重视，对恶意代码治理更投入不足。

因为多数恶意代码感染事件难以被直观地发现，但“敲诈者”以端点为侵害目标，其威胁后果则粗暴可见。同时，对于类似威胁，仅仅依靠网络拦截是不够的，必须强化端点的最后一道防线，必须强调终端防御的有效回归。安天智甲终端防御系统研发团队依托团队对“敲诈者”的分析和预判，依托安天反病毒引擎和主动防御内核，完善了多点布防，包括文档访问的进程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定等。

经过这些功能的强化，安天不仅能够有效检测防御目前“敲诈者”的样本，并能够分析其破坏机理，还对后续“敲诈者”可能使用的技巧进行了布防。同时，安天探海威胁检测系统，可对进入企业的勒索软件和漏洞利用行为进行威胁感知；安天追影威胁分析系统，针对勒索软件的防护，可采用回溯判定、分级防护的策略通过自动化判定勒索软件，并提供检出规则和特征分发到其他安全产品中。

此外，小结本次威胁的影响范围和应急处置经验教训，我们建议网络和 IT 环境复杂的大中型机构对后续的安全防护体系考虑如下优化：

1. 当前专有终端防护能力相对不足，本次事件中有相当数量的专有终端受害，建议对 ATM、各类闸机等专用终端，部署智甲专用终端防护版以增强防护能力；

2. 本次事件中大量受害用户为隔离内网，进一步体现出“过于依赖网络边界防护和物理隔离的安全体系，反而可能内部网络安全疏漏较多、安全治理工作也任重道远”，建议重视内网安全能力提升，建设内网纵深防御体系；

3. 在这次的应急工作中，我们每每感叹“缺乏有效的基于资产的安全管理、感知、和响应平台支撑时，在复杂网络的应急工作中应急人员往往有力使不出”。目前，很多用户正在规划或建设网络安全态势感知和监控预警平台，针对安全事件的汇聚、研判、以及呈现固然要重点考虑，但建议更应加强对“基于资产的安全分析、处置响应、处置进展监控”等能力的规划。

金钱夜未眠，在巨大的经济利益驱使下，未来勒索软件的传播途径和破坏方式也会变得愈加复杂和难以防范。作为安天智甲的开发者，我们期望帮助更多用户防患于未然。

从 NSA 网路军火泄露 EternalBlue 漏洞利用工具，到本次利用相关漏洞传播的勒索软件全球爆发，安天在本年度首次启动了 A 级风险预警到大规模安全风险应急。这是自心脏出血、破壳和 mirai 之后，安天又一次启动 A 级风险应急，并为本次事件逐步从 A 级安全风险提升到大规模 A 级安全灾难。

在过去几年间，类似“红色代码”、“震荡波”、“冲击波”等大规模蠕虫感染带来的网络拥塞，系统大面积异常等事件日趋减少。而对基于 PC 节点的大规模僵尸网络的关注也开始不断下降，类似 Mirai 等 IoT 僵尸网络开始成为注意力的焦点。这使传统 IT 网络开始陷入一种假想的“平静”当中。由于 Windows 自身在 DEP、ASLR 等方面的改善， 使一击必杀的系统漏洞确实在日趋减少，主流的攻击面也开始向应用开始转移。在这种表面上的平静之中，以窃密、预制为目的的 APT 攻击，则由于其是高度隐秘的、难以为 IT 资产的管理者感知到的攻击，始终未能得到足够的重视。而黑产犯罪的长尾化，针对性的特点，也使其并不依赖极为庞大的受害人群分布，即可获得稳定的黑色收益。

因此在过去几年，内网安全风险是围绕高度隐蔽性和定向性展开的，这种风险难以感知的特点，导致内网安全未得到有效的投入和重视。也为导致今天的大规模安全灾难形成了必然基础。勒索软件的一大特点，是其威胁后果是直接可见的。这种极为惨烈的损失，昭示了内网安全的欠账。也说明我们长期在简单的边界防护、物理隔离和内部的好人假定的基础上经营出安全图景，是一种“眼不见为净”式的自欺，无法通过攻击者的检验。

当前，我国在内网安全体系上的能力缺陷，一方面是安全产品未能得到全面部署和有效使用，另一方面则首先是其规划建设中没有落实“三同步”的原则，缺少基础的安全架构。

安天、360 等能力型安全厂商共同认同的滑动标尺模型，认为安全能力可以划分成架构安全、被动防御、积极防御、威胁情报等层次。各层次构成一个有机的整体，网络安全规划以基础的安全架构和可靠的被动防御手段为基础，叠加有效的积极防御和威胁情报手段。如果没有架构安全和被动防御的基础支撑，那么上层能力难以有效发挥；如果没有积极防御和威胁情报的有效引入，仅靠基础措施也无法有效的对抗深度的威胁。每个安全层次解决不同的问题，有不同的价值。相对更低的层次付出的成本更低，但解决的问题更基础广泛。从网络安全投入上看，越是网络初期越要打好底层的工作，而越是保障高等级的资产，就需要在积极防御和威胁层面做出投入延展。

习近平总书记在 4.19 网络安全与信息化工作座谈会上已经告诫我们“网络安全的威胁来源和攻击手段不断变化，那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念并特别指出了 “物理隔离”防线可被跨网入侵”等若干值得关注的安全风险。要求我们全天候全方位感知网络安全态势。

在 2 月 17 日国家安全工作座谈会上，总书记又进一步强调要“实现全天候全方位感知和有效防护”。

防护的有效性最终要在与攻击者的对抗中检验，尽管这次事件带来的损失已经是非常惨痛的，但我们需要警醒的是，相对更为深度、隐蔽的针对关键信息基础设施的攻击，这种后果可见的大规模灾难依然是一种浅层次风险。有效完善纵深防御体系和能力势在必行。

1 小时启动“A 级灾难”响应

发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》深度分析报告。

发布科普文章

针对网络高频问题、对网络传言方式验证，发布《安天应对勒索者蠕虫病毒 WannaCry FAQ-1、2》。

及时响应客户需求，开展应急服务支持

- 为政企客户等修订应急手册，增补开机指南部分。
- 利用 U 盘、光盘等工具为客户提供一站式解决方案。

为用户提供全面应急工具

- 发布配置指南：网站版、PDF 版。
- 发布开机指南：发布周一开机指南。
- 提供“体检”内网风险扫描服务。
- 提供“免疫工具”，一键关闭高危端口和进程。
- 提供“专杀工具”清除已有内网病毒，防目扩散感染。
- 发布安天智甲防勒索免费版。

安天全套防护解决方案：三重防护体系

第一重，边界防御：及时阻隔已知病毒及未知病毒，使病毒不能通过边界（U 盘拷贝、即时通讯软件传输、下载、邮件）进入终端“进不来”。

第二重，主动防御：及时阻止已知 / 未知病毒的运行“起不来”。

第三重，文档安全工具：专门针对勒索软件的工具，并在加密文档之前及时阻断勒索进程，保护用户终端文档不被加密“改不了”。

【跟进历史】

安天从 2014 年以来持续跟进分析勒索软件，先后发布多篇针对勒索软件的分析报告。安天智甲终端防御系统，通过黑白双控、动态行为监测、诱饵文件等多种方式有效拦截勒索软件的启动和加密行为，使其即使通过高级手段注入，也无法对主机文件加密。

安天探海威胁检测系统、追影威胁分析系统能有效检测分析各种新型勒索软件。安天的产品体系和态势感知系统是针对应对高级威胁设计的，应对勒索者病毒自然游刃有余。

2015 年

- 4 月 30 日，《“攻击 WPS”样本实为敲诈者》
- 8 月 3 日，《揭开勒索软件的真面目》
- 12 月 4 日，《邮件发送 JS 脚本传播敲诈者木马的分析报告》

2016 年

- 1 月 17 日，《2015 年网络安全威胁的回顾与展望》
- 2 月 19 日，《发现使首例具有中文提示的比特币勒索软件“LOCKY”》
- 12 月 20 日，《2016 网络安全威胁的回顾与展望》（安天基础威胁年报）

2017 年

- 4 月，《勒索软件简史》（《中国信息安全》2017 年第 4 期）
- 5 月 13 日 06:00 发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》
- 5 月 14 日 05:22 更新《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》

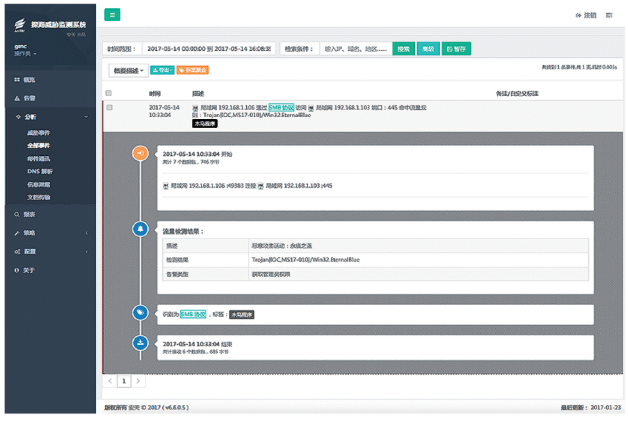
勒索者蠕虫病毒 WannaCry 专题

【产品能力】

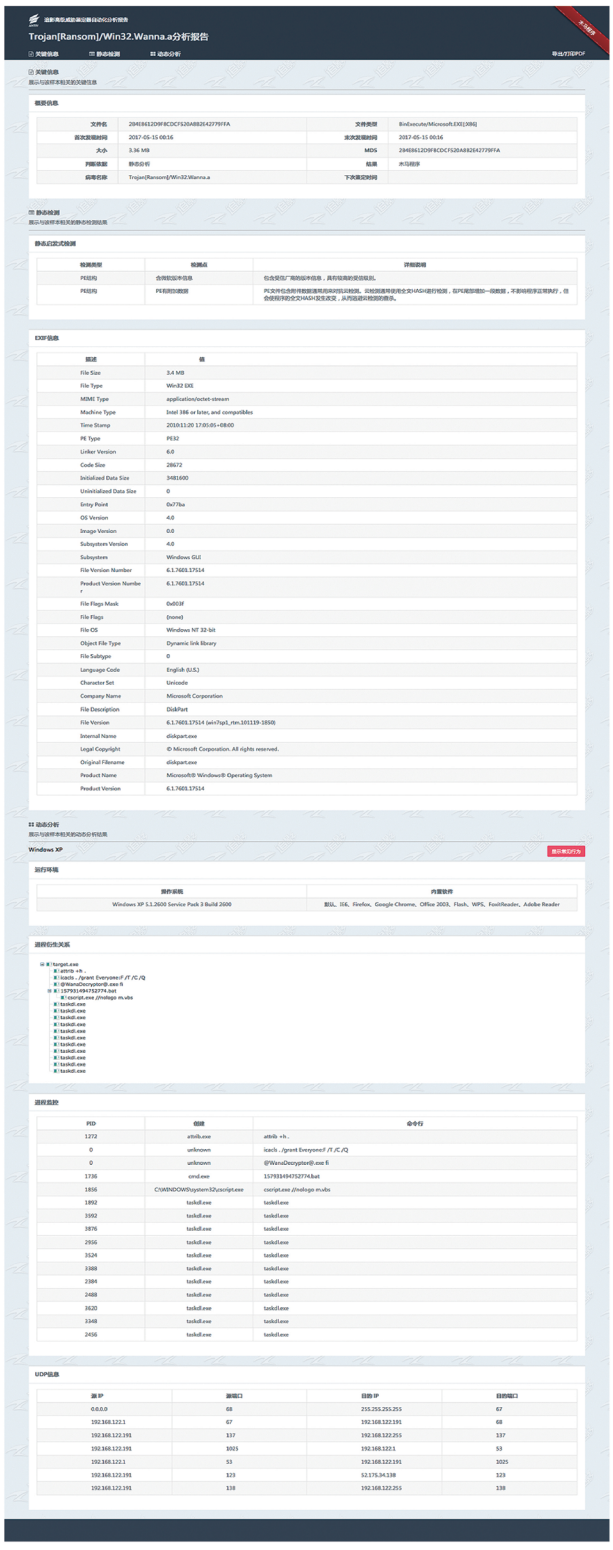
5 月 12 日，新型蠕虫式勒索软件“WannaCry”爆发，经过测试验证，安天智甲终端防御系统，此前的版本无需升级即可有效阻断 WannaCry 的加密行为；安天探海威胁检测系统可以检出 WannaCry 的扫描包（需要升级到最新特征库）；追影威胁分析系统无需升级，即可依据行为进行检出。

安天智甲免费版界面图

安天智甲终端防御系统检出图



探海威胁监测系统界面图



追影威胁分析系统实际分析截图