（上接第三版）

挖矿木马逐步泛滥，开启了新的对抗局面。这一时期的勒索软件，采用比特币作为赎金形式，采用暗网作为不可追踪的支付链路，采用 AES、RSA 等难于解密的强加密算法来加密用户数据，构成一个难以打破的“铁三角”。同时，挖矿木马也在借助虚拟货币、暗网交易等手段提升隐秘性和不可溯源性。

2010 年 3 月 9 日，安天受相关部门委托，进行了长达 2 个月的调查研究，最终呈报了《中国互联网黑色网络安全产业链情况的报告及对策》。本次调查研究基于海量终端体系呈现宏观全景视图，形成目前地下产业经济现状调查研究报告及多篇相关木马深度分析报告。该调研报告全面揭示了地下产业网络体系带给现实社会的危害，并提出简要的应对措施，旨在推动互联网产业健康、有序发展。

2015 年 8 月，安天基于多年来对各种勒索软件的深度剖析，发布了《揭开勒索软件的真面目》的报告。该报告从传播手段、表现形式、分类情况、演进历史、新的变化趋势等角度对勒索软件进行了全方位的分析，并针对不同的用户和场景提出了解决方案和建议。

2016 年 2 月 18 日，安天 CERT 发现首例具有中文提示信息的勒索软件家族，名为“Locky”。这预示着勒索软件作者针对的目标范围逐渐扩大，勒索软件将发展出更多的本地化版本。

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”的扩散将全面降低攻击者的攻击成本，以及勒索模式会不可避免地带动蠕虫的回潮等观点。结果未满 1 个月，**安天预测的“勒索软件 + 蠕虫”的传播方式即被不幸言**。2017 年 5 月 12 日晚，“魔窟”（WannaCry）勒索软件在全球范围内爆发。我国大量行业企业网络受到大规模感染。安天第一时间启动“A 级灾难响应”，第一时间上报主管部门、到达用户现场。次日凌晨 6 时，第一时间对外发布了《安天应对勒索蠕虫“魔窟”（WannaCry）的深度分析报告》，并给出了临时解决方案。此后安天持续跟进，依次发布了多篇报告及专杀、免疫和解密工具。**魔窟事件的爆发引起我们对安全防护的深思，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。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非常惨痛，但我们更需要警醒的是，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，因此，有效完善纵深防御体系和能力势在必行。**

▲勒索软件“魔窟”（WannaCry）运行流程（2017）

随后的几年里，安天 CERT 持续跟踪分析勒索软件，并发布了多个流行勒索软件报告，包括 GANDCRAB、GlobeImposter、Sodinokibi、Phobos、WannaRen、ProLock 等。

2013 年，安天用泛化（Malware/Other）一词，用以说明安全威胁向智能设备等新领域的演进——之后泛化（Malware/Other）一直被作为主要的威胁趋势，社会逐步走向“万物互联”的时代，新兴技术的高速发展导致了安全威胁的入口泛化。此时，恶意代码的影响范围已经从个人用户全面延伸至政企网络，**木马不再只是一种恶意代码类型，而成为典型的地下经济模式**。

2015 年 9 月，发生了一例 Xcode 非官方版本恶意代码污染事件，这一事件称为“XcodeGhost”。Xcode 是由苹果公司发布的运行在操作系统 Mac OS X 上的集成开发工具（IDE），是开发 Mac OS 和 iOS 应用程序的主流工具。攻击者通过对 Xcode 进行篡改，加入恶意模块，并进行各种传播活动，致使大量开发者使用被污染过的版本建立开发环境。鉴于此事态的严重性，安天 CERT 与安天移动安全公司组成联合分析小组，分析并发布了该事件的报告。

2016 年 10 月 22 日下午，安天针对美国东海岸 DNS 服务商 Dyn 遭遇 DDoS 攻击事件进行了跟进分析。该事件涉及到 IoT（Internet of Things，物联网）设备安全等多种因素，这也印证了 2015 年安天论述的“威胁将随‘互联网 +’向纵深领域扩散与泛化”的观点，**正如我们所担心的那样，从智能穿戴、智能家居、智能汽车到智慧城市，安全威胁已经无所不在。**

▲Xcode 非官方供应链污染事件示意图（2015）

2019 年，WannaMine 挖矿木马爆发，同年 5 月，安天接到某重要单位的求助，其内网中执行任务的上百台主机频繁出现死机、重启、蓝屏等现象。用户部署使用的某款杀毒软件能查出恶意代码告警，但显示成功清除后，恶意代码很快又会重新出现。安天接到求助于当日傍晚飞抵客户现场进行处置，快速解决了问题，并随后发布响应报告《**六小时处置挖矿蠕虫的内网大规模感染事件**》。

**近十年，安天 CERT 依托大规模自动化分析处理体系的逆向分析、关联分析、同源分析等平台，发布了大量分析报告，打造了“第一时间启动，同时应对多线威胁，三体系联动，四作业面协同”的应急体系**。

安天 CERT 对勒索软件进行了大量的分析与研究，从防御视角看，针对勒索软件的防护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，必须回归到有效的终端防御。安天持续跟进研究勒索软件威胁机理，采集归纳了近百种勒索软件行为特征，形成了多个规则启发式勒索软件检测模式。面对 2017 年 5 月爆发的魔窟事件，2016 年 1 月版本的安天智甲即可实现有效防护。安天智甲终端防御系统（IEP）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。

下期《安天周观察》将连载文章
《从反恶意代码到对抗高级威胁（下）》
或微信扫描二维码关注安天微信公众号阅读全文

安天周观察
安天官方微博　安天官方微信
主办：安天　2020 年 6 月 22 日 ( 总第 235 期 ) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

# 从反恶意代码到对抗高级威胁（上）

威胁是一场你争我夺的战争；能力是一场新我与旧我的迭代；告别与迎接是一道暗示自己的口令；20 年的安全威胁，不是亲历者的功成身退，而恰是眼前蓄势待发的动力。一文记录网络安全 20 载的威胁事件，读一个企业的磨砺与坚持，阅一条道路的来处与前程。

## 概述

安天团队创业于 2000 年，经历了以民间技术实验室为模式的十年和企业化运营的十年。无论运营模式如何变化，安天始终站在威胁对抗的第一线。过去的二十年正是信息化高速发展、安全威胁剧烈演进的二十年。安天因需而变，不断完善威胁监测、捕获能力，建立起包括流量监测、蜜罐捕获、诱饵信箱、情报共享等十余环节在内的前端感知体系；不断提高自动化分析与处置能力，逐步建立起日处理量达百万级以上的自动化处理平台，形成了超大规模的威胁知识图谱和安天 TID 威胁情报平台。在从红色代码到“魔窟”（WannaCry）等重大安全事件对抗的过程中，安天逐步形成了“第一时间启动，同时应对多线威胁，三体系联动，四作业面协同”的应急响应机制。

当前，网络空间领域的斗争已经是大国博弈和地缘安全中常态化的存在，网络空间更是政治、军事、经济等领域斗争的首发“战场”，能力型网络安全企业需要不断提高对自身的使命要求。自 2010 年起，安天深度跟进多个 APT（高级持续性威胁）攻击事件和攻击组织，并结合 TID 威胁情报平台和追影威胁分析系统等产品展开大量分析工作，发布了多篇重量级分析报告，揭示我国所遭受到的 APT 攻击。

安天正从过去与恶意代码对抗的小闭环，走向全面赋能客户和助力客户建设防御体系、有效对抗威胁的大闭环。对安天来说，这是一个艰难的过程，也是必须实现的突破。

本文是安天对过去 20 年来与安全威胁对抗过程的回顾与反思，我们将带着持续的技术积累和自我反思，面对着更加明确的责任使命再上征程。朝花夕拾回看来路，风雨兼程不负初心。

## 捕影廿载——流行性威胁 20 年应急响应事件回顾

2000 年在信息技术发展是一个特殊的时点，个人计算机革命的高潮与信息高速公路的兴起叠加激荡。单机操作系统 DOS 全面退场，全面支持网络通信的 Windows 9x 操作系统的广泛使用；Windows NT 也在全面蚕食着传统 UNIX 的市场，WEB 服务、FTP 服务、电子邮件服务，从象牙塔中的奢侈品，变成普通用户获取和交换信息的方式。这种变化在带来巨大革命变革的同时，计算机恶意代码也借此大规模流行。

在 DOS 时代，感染式病毒（Virus）、蠕虫（Worm）和特洛伊木马（Trojan），都是相对窄带而互斥的技术概念。从形态上看，感染式病毒是一个代码片断，需要感染宿主程序或磁盘引导记录，蠕虫是不感染宿主程序而传播自身的独立程序，木马则是指预设恶意逻辑但不具备传播能力的程序。在此时期，磁盘是数据交换的主要方式，感染式病毒从种类和数量来看，都居于主流地位。这一情况随着 Win9x 系统兴起发生了巨变：恶意代码编写者的想象力突破了程序宿主空间的限制，Happy99 蠕虫利用劫持电子邮件的方式传播并快速流行，拉开了蠕虫时代大幕；代号“死牛祭礼”（Cult of the Dead Cow）的黑客组织发布了 Back Orifice 2000 木马（简称 BO）并将其开源，BO 随即成为国内划时代的网络攻击工具，并从此激活了特洛伊木马中最为庞大的分支——RAT（Remote Access Trojan，远程控制木马）。

在此后的恶意代码演进中，感染式病毒日渐式微，蠕虫成为主流威胁类型并延续 5~8 年时间。其后，特洛伊木马数量在利益驱动的模式下开始呈几何级数增长。此时，“病毒”从狭义的感染式病毒概念已经转化为对各种恶意程序的统称，并被媒体所广泛使用，但在学术文献中，则以恶意代码（Malicious code，简称 Malware）概念来表示上述各种威胁。

### ●蠕虫大爆发时代（2000~2005）

2001 年 8 月 6 日，红色代码蠕虫变种“红色代码 II”（CodeRedII）在国内爆发，安天第一时间启动应急响应。红色代码完全超出了传统反病毒工作者的常规认知，蠕虫没有文件载体，而是依靠 IIS 服务的溢出漏洞传播，并在系统内存中存活——蠕虫进入系统后，会创建一个恶意文件，但这个恶意文件被用于构造后门，而非蠕虫的文件实体。安天在国内部分 IDC 主机部署的监测探针在第一时间发现了红色代码 II 的端口扫描行为，病毒分析组（现为安天安全研究与应急处理中心，简称安天 CERT）立即进行分析。6 小时后安天公开发布分析报告、提供专杀工具，并协助主管部门开发了扫描排查工具。

2002 年，安天开始与哈工大相关教研室共同开展反病毒方向研究，并组建了哈工大 - 安天联合 CERT 小组。在此期间，安天研发出适用于高速网络的具备全规则过滤能力的反病毒引擎。

2003 年 3 月 8 日，哈工大 - 安天联合 CERT 小组在多个监控节点发现异常网络行为，并采集到后来被命名为口令蠕虫（Dvldr）的恶意代码样本。联合小组紧急启动样本分析和事件处置工作，发布专杀、验证工具和免疫工具。此后，联合小组通过近 3 个月的分析溯源，排查出国内 4.7 万个感染节点，并还原了部分的传播时序。

安天 CERT 刚刚起步时，在只有几名

（下转第三版）

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | NHS 披露 113 个内部电子邮件账户遭到黑客入侵 |
| 英文标题 | NHS: 100+ Email Accounts Hijacked in Phishing Campaign |
| 作者及单位 | Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine |
| 内容概述 | NHS 已经证实，大约两周前，有 113 个内部电子邮件账户被入侵，并被用来向健康服务之外发送恶意垃圾邮件。周五发布的一份简短的 NHS 数字声明显示，该事件发生在 2020 年 5 月 30 日星期六到 6 月 1 日星期一之间。该公司称，此次安全故障只影响了“非常小的一部分”NHS 电子邮件账户，约占总数 140 万的 0.008%，并与一场旨在窃取受害者登录信息的更大范围活动有关。目前没有证据表明患者的病历被访问过。 |
| 链接地址 | https://www.infosecurity-magazine.com/news/nhs-100-email-accounts-hijacked/ |

## 每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

| 恶意代码类别 | 名称与发现时间 | 威胁等级 | 简要描述 |
|---|---|---|---|
| 活跃漏洞 | Microsoft Excel 资源管理错误漏洞（CVE-2020-0901） | 高 | 当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。与拥有管理员权限的用户相比，帐户被配置为拥有较少权限的用户受到的影响更小。 |
| | Microsoft Internet Explorer 安全漏洞（CVE-2020-1062） | 高 | 当 Internet Explorer 不正确地访问内存中的对象时，会触发远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。 |
| | Microsoft Windows Jet Database Engine 安全漏洞（CVE-2020-1174） | 高 | 当 Windows Jet 数据库引擎不正确地处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。 |
| 较为活跃样本家族 | Virus/Win32.Nimnul | 中 | 此威胁是一种感染类病毒家族。该家族样本主要感染 exe 和 html 文件。被感染的文件运行时，首先释放并运行恶意文件，然后再运行正常文件。该家族文件具有 hook 系统函数、注入 DLL、创建启动项、等待连网控制、感染可移动存储介质等功能。 |
| | Virus/Win32.Lamer | 中 | 此威胁是一种感染式病毒家族。该感染式病毒在感染文件时将自身代码放置到被感染程序的前面，属于前置型感染。通常这个家族在感染程序前还将微软文档转换文件 write32.wpc 一同放置到被感染程序前，是这感染式病毒中极为少见的一种行为。 |
| | Trojan[Packed]/Win32.Krap | 中 | 此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。 |
| | Trojan/Win32.Bayrob | 中 | 此威胁是一种可以窃密类木马家族。该家族样本运行后连接远程服务器，收集用户敏感信息并回传，包括操作系统版本、计算机名、计算机的 IP 地址、关于操作系统和系统设置的信息、MAC 地址及运行服务列表等。 |
| | Trojan/Win32.Kryptik | 中 | 此威胁是一种可以窃密类木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键信息，并回传服务器。 |
| | Trojan/Android.catwatchful | 中 | 此威胁是一种间谍类木马家族。该家族木马运行后隐藏图标，后台窃取用户短信、联系人、通话记录、地理位置等隐私信息，私自拍照、录音、录像。并将用户隐私上传至指定邮箱，造成用户隐私泄露。 |
| | Trojan/Android.BankBot | 中 | 此威胁是一种银行木马家族，该家族木马运行后请求激活设备管理器，隐藏图标，上传用户隐私信息，还会接收指令下载未知 apk 诱导用户安装，造成用户隐私泄露和资费损耗。 |



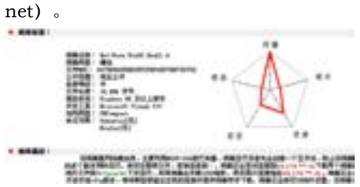
（上接第一版）

分析人员的情况下，先后完成了多个重大事件的分析任务。在不断的取证、分析、溯源实战中，安天 CERT 逐渐成长，经历的磨练和积累的经验**为日后的应急响应工作流程奠定了坚实的基础**。

▲安天对于蠕虫类威胁事件的应急处理流程（2004）

从产品技术变革上的角度看，这一时期是由蠕虫事件驱动着网络侧产品技术的发展。2000 年初，网络威胁以 happy99 等邮件蠕虫、CodeRed 为代表的扫描溢出型蠕虫为主。但此时网络监测设备的载体的处理能力并不乐观，直路设备的吞吐量仍以百兆级别为主；所能检测、过滤的对象主要在数据包报头层次，而非内容，遑论流量的完整还原；旁路设备实现流量还原所需的并行协议栈等技术亦不成熟。**安天从 2002 年起，尝试在包层次构建不依赖预处理器的全规则引擎，并达到千兆的线速，使反病毒引擎突破了必须依赖协议还原进行文件检测的局限，可以适配千兆零拷贝技术**。2004 年，安天将使用这一引擎的流量检测系统命名为 VDS（即网络病毒检测系统），**系统基于旁路接入方式，针对网络侧的流量进行还原与检测。该系统为我国监测大规模恶意代码活动奠定了技术基础，安天探海威胁检测系统正是在该系统的基础上研发而成**。

**安天在恶意代码分析工作中推动了恶意代码知识的体系化完善，形成了恶意代码百科全书，并提供公众查询**（Virusview.net）。



▲安天病毒百科全书（2005）

### ●木马泛滥时代（2005~2010）

2005 年开始，0day 漏洞逐渐被攻击者用于定向攻击或批量投放恶意代码，而不再被用于编写蠕虫；端点系统的安全性随着 WindowsXP 等系统的广泛应用得到一定程度的提升，DEP、ALSR 等保护技术成为系统的默认安全配置。网络蠕虫的影响趋向衰弱，特洛伊木马的数量开始呈爆炸式增长。随着社交软件、网络游戏用户量持续增加，恶意代码作者的逐利性取代了炫技、心理满足、窥视隐私等网络攻击活动的原生动力，成为网络攻击活动的主要意图。通过窃取网络凭证、游戏账号、虚拟货币等方式的获利行为开始普遍化。此类恶意代码隐匿在计算机中进行窃密活动，很像古希腊特洛伊战争中著名的“木马计”。

2005 年，以灰鸽子为代表的远程控制程序在技术上趋于成熟，感染数量持续增加，安天 CERT 对这类远程控制程序进行了大量的分析和研究，并协助相关部门通过网络开展远程控制程序的使用情况的监测工作。2006 年 6 月 9 日，安天捕获到国内首个以敲诈为目的的 Redplus 木马，**该恶意代码正是今天日益泛滥的勒索软件的雏形**。同年 8 月 14 日，在魔波（Mocbot）事件中，安天在 3 小时内完成初步分析，及时发布了警报和分析报告，提供专杀工具，全面阻止魔波病毒在我国肆虐，快速清除了国内感染的病毒。同年熊猫烧香爆发，在短时间内感染全球大量计算机，受害主机的可执行文件的图标都被改为熊猫举着三根香的模样。安天 CERT 对熊猫烧香不同变种的传播方式、感染方式等进行了及时分析，并快速发布了专杀及修复工具。

2007 年至 2009 年地下经济运作日趋“成熟”，使恶意代码不再只是属于民间，而是更加向着“职业技术团队”方向发展开发和研究，在此技术支撑下，形成了一条灰色的产业链。此阶段各类木马猖獗，迎来爆发的高峰期，传播范围尤其广泛。而以熊猫烧香为代表的蠕虫恶意代码也开始在这个阶段渐渐消退，退出历史的舞台。随着社交软件、网络游戏的兴盛，窃取网络凭证、游戏账号、虚拟货币类的恶意代码开始流行。另外广告件、僵尸网络、下载者（Downloader）等恶意代码也“遍地开花”。盗取账号类主要以盗取 QQ 凭证（QQpass 家族）、网络游戏凭证（OnlineGames 家族）为主，传播方式主要以网页挂马、U 盘为主。此时期杀毒软件开始强化针对网络游戏盗号木马的监测查杀，随后“AV 终结者”木马爆发，该木马当选 2007 上半年的“毒王”。AV 终结者其主要特征是通过 U 盘传播，与杀毒软件等相关安全程序对抗，破坏安全模式，下载大量盗号木马，其变种能够破坏磁盘免疫。安天在 2007 至 2009 年间分析了大量流行木马。

木马数量的激增催化了后端分析支撑体系的完善。反恶意代码技术如同一座冰山，引擎和前端产品只是冰山水面之上的部分，而其更庞大的部分——恶意代码后台分析处理机制——则在水面之下，这是一个庞大的基于大量计算节点形成的分布式处理体系。2005 年起，一方面是互联网广泛普及拉动应用程序数量快速增长，另一方面则是地下经济活动猖獗拉动木马数量急剧膨胀，反病毒厂商每日捕获到的未知文件数量迅速由万量级提升到十万、百万量级。巨大的样本辨识压力横亘在反病毒工作者面前，**全面采用人工分析响应将导致工作量趋向不可收敛**。安天在现有批量样本自动化分析流水线基础上，开始筹划建立和完善面向**海量样本的自动化流水线分析平台**，通过引入虚拟执行分析、格式识别和深度静态拆解、对照扫描、文件信誉度检测、终端信誉度检测等方法，使整个体系的鉴定能力逐步得到提升，可以对全量文件实现自动化的“鉴定 - 规则 - 检测”的循环，只把少数疑难样本留给人工处理，**最终解决了样本数量激增和分析人员不足而产生的瓶颈，显著提升了分析效率**。

▲自动化流水线分析平台（2005）

### ●虚拟货币和隐秘网络带动的勒索新对抗（2010~2020）

2010 年前后，恶意代码已经完全产业化，通过与地下经济体系深度融合，形成了新的威胁形态。早期盗号木马、广告点击器、浏览器首页锁定器这类恶意代码虽然严重危害系统安全，却并不会导致系统直接停摆，但自 2013 年开始，勒索软件、

（下转第四版）